BULLETIN (SB24-057)

VULNERABILITY SUMMARY FOR THE MONTH OF

FEBRUARY 2024

Bulletin (SB24-057)
Vulnerability Summary for the Month of February 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
agronholm -- cbor2	cbor2 provides encoding and decoding for the Concise Binary Object Representation (CBOR) (RFC 8949) serialization format. Starting in version 5.5.1 and prior to version 5.6.2, an attacker can crash a service using cbor2 to parse a CBOR binary by sending a long enough object. Version 5.6.2 contains a patch for this issue.	2024-02-19	7.5	CVE-2024-26134
alfio-event -- alf.io	alf.io is an open source ticket reservation system. Prior to version 2.0-Mr-2402, organization owners can view the generated API KEY and USERS of other organization owners using the `http://192.168.26.128:8080/admin/api/users/<user_id>` endpoint, which exposes the details of the provided user ID. This may also expose the API KEY in the username of the user. Version 2.0-M4-2402 fixes this issue.	2024-02-19	8.8	CVE-2024-25635
alfio-event -- alf.io	alf.io is an open source ticket reservation system. Prior to version 2.0-Mr-2402, an attacker can access data from other organizers. The attacker can use a specially crafted request to receive the e-mail log sent by other events. Version 2.0-M4-2402 fixes this issue.	2024-02-19	7.2	CVE-2024-25634
anton_kueltz -- fastecdsa	Versions of the package fastecdsa before 2.3.2 are vulnerable to Use of Uninitialized Variable on the stack, via the curvemath_mul function in src/curveMath.c, due to being used and interpreted as user-defined type. Depending on the variable's actual value it could be arbitrary free(), arbitrary realloc(), null pointer dereference and other. Since the stack can be controlled by the attacker, the vulnerability could be used to corrupt allocator structure, leading to possible heap exploitation. The attacker could cause denial of service by exploiting this vulnerability.	2024-02-24	7.5	CVE-2024-21502
areal_topkapi -- webserv2	An unauthenticated remote attacker can bypass the brute force prevention mechanism and disturb the webservice for all users.	2024-02-22	7.5	CVE-2024-1104
b&r_industrial_automation -- automation_studio	B&R Automation Studio Upgrade Service and B&R Technology Guarding use insufficient cryptography for communication to the upgrade and the licensing servers. A network-based attacker could exploit the vulnerability to execute arbitrary code on the products or sniff sensitive data. Missing Encryption of Sensitive Data, Cleartext Transmission of Sensitive Information, Improper Control of Generation of Code ('Code Injection'), Inadequate Encryption Strength vulnerability in B&R Industrial Automation B&R Automation Studio (Upgrade Service modules), B&R Industrial Automation Technology Guarding.This issue affects B&R Automation Studio: <4.6; Technology Guarding: <1.4.0.	2024-02-22	8.3	CVE-2024-0220
backstage -- backstage	`@backstage/backend-common` is a common functionality library for backends for Backstage, an open platform for building developer portals. In `@backstage/backend-common` prior to versions 0.21.1, 0.20.2, and 0.19.10, paths checks with the `resolveSafeChildPath` utility were not exhaustive enough, leading to risk of path traversal vulnerabilities if symlinks can be injected by attackers. This issue is patched in `@backstage/backend-common` versions 0.21.1, 0.20.2, and 0.19.10.	2024-02-23	8.7	CVE-2024-26150
brivo -- acs100,_acs300	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Brivo ACS100, ACS300 allows OS Command Injection, Bypassing Physical Security.This issue affects ACS100 (Network Adjacent Access), ACS300 (Physical Access): from 5.2.4 before 6.2.4.3.	2024-02-19	9	CVE-2023-6260
brivo -- acs100,_acs300	Insufficiently Protected Credentials, : Improper Access Control vulnerability in Brivo ACS100, ACS300 allows Password Recovery Exploitation, Bypassing Physical Security.This issue affects ACS100, ACS300: from 5.2.4 before 6.2.4.3.	2024-02-19	7.1	CVE-2023-6259
code-projects -- crime_reporting_system	A vulnerability was found in code-projects Crime Reporting System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file inchargelogin.php. The manipulation of the argument email/password 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-254608.	2024-02-23	7.3	CVE-2024-1820
code-projects -- library_system	A vulnerability has been found in code-projects Library System 1.0 and classified as critical. This vulnerability affects unknown code of the file Source/librarian/user/student/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-254614 is the identifier assigned to this vulnerability.	2024-02-23	7.3	CVE-2024-1826
code-projects -- library_system	A vulnerability was found in code-projects Library System 1.0 and classified as critical. This issue affects some unknown processing of the file Source/librarian/user/teacher/login.php. The manipulation of the argument username/password leads to sql injection. The attack may be initiated remotely.	2024-02-23	7.3	CVE-2024-1827

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-254615.			
code-projects -- library_system	A vulnerability was found in code-projects Library System 1.0. It has been classified as critical. Affected is an unknown function of the file Source/librarian/user/teacher/registration.php. The manipulation of the argument email/idno/phone/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-254616.	2024-02-23	7.3	CVE-2024-1828
code-projects -- library_system	A vulnerability was found in code-projects Library System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file Source/librarian/user/student/registration.php. The manipulation of the argument email/regno/phone/username 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-254617 was assigned to this vulnerability.	2024-02-23	7.3	CVE-2024-1829
code-projects -- library_system	A vulnerability was found in code-projects Library System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file Source/librarian/user/student/lost-password.php. The manipulation of the argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-254618 is the identifier assigned to this vulnerability.	2024-02-23	7.3	CVE-2024-1830
codeastro -- house_rental_management_system	A vulnerability, which was classified as critical, has been found in CodeAstro House Rental Management System 1.0. Affected by this issue is some unknown functionality of the file signing.php. The manipulation of the argument uname/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-254612.	2024-02-23	7.3	CVE-2024-1824
connectwise -- screenconnect	ConnectWise ScreenConnect 23.9.7 and prior are affected by an Authentication Bypass Using an Alternate Path or Channel vulnerability, which may allow an attacker direct access to confidential information or critical systems.	2024-02-21	10	CVE-2024-1709
connectwise -- screenconnect	ConnectWise ScreenConnect 23.9.7 and prior are affected by path-traversal vulnerability, which may allow an attacker the ability to execute remote code or directly impact confidential data or critical systems.	2024-02-21	8.4	CVE-2024-1708
demososo -- dm_enterprise_website_building_system	A vulnerability has been found in Demososo DM Enterprise Website Building System up to 2022.8 and classified as critical. Affected by this vulnerability is the function dmlogin of the file indexDM_load.php of the component Cookie Handler. The manipulation of the argument is_admin with the input y leads to improper authentication. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-254605 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-23	7.3	CVE-2024-1817
discourse -- discourse-microsoft-auth	`discourse-microsoft-auth` is a plugin that enables authentication via Microsoft. On sites with the `discourse-microsoft-auth` plugin enabled, an attack can potentially take control of a victim's Discourse account. Sites that have configured their application's account type to any options other than `Accounts in this organizational directory only (O365 only - Single tenant)` are vulnerable. This vulnerability has been patched in commit c40665f44509724b64938c85def9fb2e79f62ec8 of `discourse-microsoft-auth`. A `microsoft_auth:revoke` rake task has also been added which will deactivate and log out all users that have connected their accounts to Microsoft. User API keys as well as API keys created by those users will also be revoked. The rake task will also remove the connection records to Microsoft for those users. This will allow affected users to re-verify their account emails as well as reconnect their Discourse account to Microsoft for authentication. As a workaround, disable the `discourse-microsoft-auth` plugin by setting the `microsoft_auth_enabled` site setting to `false`. Run the `microsoft_auth:log_out_users` rake task to log out all users with associated Microsoft accounts.	2024-02-21	9	CVE-2023-46241

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dromara -- hertzbeat	Hertzbeat is a real-time monitoring system. In `CalculateAlarm.java`, `AviatorEvaluator` is used to directly execute the expression function, and no security policy is configured, resulting in AviatorScript (which can execute any static method by default) script injection. Version 1.4.1 fixes this vulnerability.	2024-02-22	9.8	CVE-2023-51388
dromara -- hertzbeat	Hertzbeat is a real-time monitoring system. At the interface of `/define/yml`, SnakeYAML is used as a parser to parse yml content, but no security configuration is used, resulting in a YAML deserialization vulnerability. Version 1.4.1 fixes this vulnerability.	2024-02-22	9.8	CVE-2023-51389
dromara -- hertzbeat	Hertzbeat is a real-time monitoring system. In the implementation of `JmxCollectImpl.java`, `JMXConnectorFactory.connect` is vulnerable to JNDI injection. The corresponding interface is `/api/monitor/detect`. If there is a URL field, the address will be used by default. When the URL is `service:jmx:rmi:///jndi/rmi://xxxxxxx:1099/localHikari`, it can be exploited to cause remote code execution. Version 1.4.1 contains a fix for this issue.	2024-02-22	9.8	CVE-2023-51653
electron-pdf -- electron-pdf	electron-pdf version 20.0.0 allows an external attacker to remotely obtain arbitrary local files. This is possible because the application does not validate the HTML content entered by the user.	2024-02-20	7.5	CVE-2024-1648
eprosima -- fast-dds	eProsima Fast DDS (formerly Fast RTPS) is a C++ implementation of the Data Distribution Service standard of the Object Management Group. Even with the application of SROS2, due to the issue where the data (`p[UD]`) and `guid` values used to disconnect between nodes are not encrypted, a vulnerability has been discovered where a malicious attacker can forcibly disconnect a Subscriber and can deny a Subscriber attempting to connect. Afterwards, if the attacker sends the packet for disconnecting, which is data (`p[UD]`), to the Global Data Space (`239.255.0.1:7400`) using the said Publisher ID, all the Subscribers (Listeners) connected to the Publisher (Talker) will not receive any data and their connection will be disconnected. Moreover, if this disconnection packet is sent continuously, the Subscribers (Listeners) trying to connect will not be able to do so. Since the initial commit of the `SecurityManager.cpp` code (`init`, `on_process_handshake`) on Nov 8, 2016, the Disconnect Vulnerability in RTPS Packets Used by SROS2 has been present prior to versions 2.13.0, 2.12.2, 2.11.3, 2.10.3, and 2.6.7.	2024-02-19	9.6	CVE-2023-50257
felixschwarz -- mjml-python	The `mjml` PyPI package, found at the `FelixSchwarz/mjml-python` GitHub repo, is an unofficial Python port of MJML, a markup language created by Mailjet. All users of `FelixSchwarz/mjml-python` who insert untrusted data into mjml templates unless that data is checked in a very strict manner. User input like `&lt;script&gt;` would be rendered as `<script>` in the final HTML output. The attacker must be able to control some data which is later injected in an mjml template which is then send out as email to other users. The attacker could control contents of email messages sent through the platform. The problem has been fixed in version 0.11.0 of this library. Versions before 0.10.0 are not affected by this security issue. As a workaround, ensure that potentially untrusted user input does not contain any sequences which could be rendered as HTML.	2024-02-22	8.2	CVE-2024-26151
fortinet -- fortimanager	A relative path traversal in Fortinet FortiManager version 7.4.0 and 7.2.0 through 7.2.3 and 7.0.0 through 7.0.8 and 6.4.0 through 6.4.12 and 6.2.0 through 6.2.11 allows attacker to execute unauthorized code or commands via crafted HTTP requests.	2024-02-20	8.8	CVE-2023-42791
fortinet -- fortios	A null pointer dereference in Fortinet FortiOS version 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.12, 6.2.0 through 6.2.14, 6.0.0 through 6.0.16, FortiProxy 7.2.0 through 7.2.3, 7.0.0 through 7.0.10, 2.0.0 through 2.0.12, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7 allows attacker to denial of service via specially crafted HTTP requests.	2024-02-22	7.5	CVE-2023-29180
fortinet -- fortipam	A use of externally-controlled format string in Fortinet FortiOS 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.12, 6.2.0 through 6.2.14, 6.0.0 through 6.0.16, FortiProxy 7.2.0 through 7.2.4, 7.0.0 through 7.0.10, 2.0.0 through 2.0.12, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7, FortiPAM 1.0.0 through 1.0.3 allows attacker to execute unauthorized code or commands via specially crafted command.	2024-02-22	8.8	CVE-2023-29181
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.9 before 16.9.1. A crafted payload added to the user profile page could lead to a stored XSS on the client side, allowing attackers to perform arbitrary actions on behalf of victims."	2024-02-22	8.7	CVE-2024-1451
gitlab -- gitlab	An authorization bypass vulnerability was discovered in GitLab affecting versions 15.1 prior to 16.7.6, 16.8 prior to 16.8.3, and 16.9 prior to 16.9.1. A developer could bypass CODEOWNERS approvals by creating a merge conflict.	2024-02-22	7.7	CVE-2024-0410

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gofiber -- fiber	Fiber is a web framework written in go. Prior to version 2.52.1, the CORS middleware allows for insecure configurations that could potentially expose the application to multiple CORS-related vulnerabilities. Specifically, it allows setting the Access-Control-Allow-Origin header to a wildcard (`*`) while also having the Access-Control-Allow-Credentials set to true, which goes against recommended security best practices. The impact of this misconfiguration is high as it can lead to unauthorized access to sensitive user data and expose the system to various types of attacks listed in the PortSwigger article linked in the references. Version 2.52.1 contains a patch for this issue. As a workaround, users may manually validate the CORS configurations in their implementation to ensure that they do not allow a wildcard origin when credentials are enabled. The browser fetch api, as well as browsers and utilities that enforce CORS policies, are not affected by this.	2024-02-21	9.4	CVE-2024-25124
helm -- helm	Helm is a package manager for Charts for Kubernetes. Versions prior to 3.14.2 contain an uninitialized variable vulnerability when Helm parses index and plugin yaml files missing expected content. When either an `index.yaml` file or a plugins `plugin.yaml` file were missing all metadata a panic would occur in Helm. In the Helm SDK, this is found when using the `LoadIndexFile` or `DownloadIndexFile` functions in the `repo` package or the `LoadDir` function in the `plugin` package. For the Helm client this impacts functions around adding a repository and all Helm functions if a malicious plugin is added as Helm inspects all known plugins on each invocation. This issue has been resolved in Helm v3.14.2. If a malicious plugin has been added which is causing all Helm client commands to panic, the malicious plugin can be manually removed from the filesystem. If using Helm SDK versions prior to 3.14.2, calls to affected functions can use `recover` to catch the panic.	2024-02-21	7.5	CVE-2024-26147
hitachi -- hitachi_global_link_manager	Expression Language Injection vulnerability in Hitachi Global Link Manager on Windows allows Code Injection.This issue affects Hitachi Global Link Manager: before 8.8.7-03.	2024-02-20	7.6	CVE-2024-0715
ibm -- aix	IBM AIX 7.3, VIOS 4.1's Perl implementation could allow a non-privileged local user to exploit a vulnerability to execute arbitrary commands. IBM X-Force ID: 281320.	2024-02-22	8.4	CVE-2024-25021
ibm -- aspera_console	IBM Aspera Console 3.4.0 through 3.4.2 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 239079.	2024-02-23	8.6	CVE-2022-43842
imaging_data_commons -- libdicom	A use-after-free vulnerability exists in the DICOM Element Parsing as implemented in Imaging Data Commons libdicom 1.0.5. A specially crafted DICOM file can cause premature freeing of memory that is used later. To trigger this vulnerability, an attacker would need to induce the vulnerable application to process a malicious DICOM image.The Use-After-Free happens in the `parse_meta_element_create()` parsing the elements in the File Meta Information header.	2024-02-20	8.1	CVE-2024-24793
imaging_data_commons -- libdicom	A use-after-free vulnerability exists in the DICOM Element Parsing as implemented in Imaging Data Commons libdicom 1.0.5. A specially crafted DICOM file can cause premature freeing of memory that is used later. To trigger this vulnerability, an attacker would need to induce the vulnerable application to process a malicious DICOM image.The Use-After-Free happens in the `parse_meta_sequence_end()` parsing the Sequence Value Represenations.	2024-02-20	8.1	CVE-2024-24794
internet_computer -- agent-js	Impact: The library offers a function to generate an ed25519 key pair via Ed25519KeyIdentity.generate with an optional param to provide a 32 byte seed value, which will then be used as the secret key. When no seed value is provided, it is expected that the library generates the secret key using secure randomness. However, a recent change broke this guarantee and uses an insecure seed for key pair generation. Since the private key of this identity (535yc-uxytb-gfk7h-tny7p-vjkoe-i4krp-3qmcl-uqfgr-cpgej-yqtjq-rqe) is compromised, one could lose funds associated with the principal on ledgers or lose access to a canister where this principal is the controller.	2024-02-21	9.1	CVE-2024-1631
kedi -- electroncord	kedi ElectronCord is a bot management tool for Discord. Commit aaaeaf4e6c99893827b2eea4dd02f755e1e24041 exposes an account access token in the `config.json` file. Malicious actors could potentially exploit this vulnerability to gain unauthorized access to sensitive information or perform malicious actions on behalf of the repository owner. As of time of publication, it is unknown whether the owner of the repository has rotated the token or taken other mitigation steps aside from informing users of the situation.	2024-02-20	7.5	CVE-2024-26136
liferay -- portal	Reflected cross-site scripting (XSS) vulnerability in the instance settings for Accounts in Liferay Portal 7.4.3.44 through 7.4.3.97, and Liferay DXP 2023.Q3 before patch 6, and 7.4 update 44 through 92 allows remote attackers to inject	2024-02-21	9	CVE-2023-40191

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary web script or HTML via a crafted payload injected into the "Blocked Email Domains" text field			
liferay -- portal	Reflected cross-site scripting (XSS) vulnerability on the add assignees to a role page in Liferay Portal 7.3.3 through 7.4.3.97, and Liferay DXP 2023.Q3 before patch 6, 7.4 GA through update 92, and 7.3 before update 34 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_roles_admin_web_portlet_RolesAdminPortlet_tabs2 parameter.	2024-02-21	9.6	CVE-2023-42496
liferay -- portal	Reflected cross-site scripting (XSS) vulnerability in the Language Override edit screen in Liferay Portal 7.4.3.8 through 7.4.3.97, and Liferay DXP 2023.Q3 before patch 5, and 7.4 update 4 through 92 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_portal_language_override_web_internal_portlet_PLOPortlet_key parameter.	2024-02-21	9.6	CVE-2023-42498
liferay -- portal	Stored cross-site scripting (XSS) vulnerability in the Document and Media widget in Liferay Portal 7.4.3.18 through 7.4.3.101, and Liferay DXP 2023.Q3 before patch 6, and 7.4 update 18 through 92 allows remote authenticated users to inject arbitrary web script or HTML via a crafted payload injected into a document's "Title" text field.	2024-02-21	9	CVE-2023-47795
liferay -- portal	Cross-site scripting (XSS) vulnerability in HtmlUtil.escapeJsLink in Liferay Portal 7.2.0 through 7.4.1, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 15, and older unsupported versions allows remote attackers to inject arbitrary web script or HTML via crafted javascript: style links.	2024-02-21	9.6	CVE-2024-25147
liferay -- portal	Stored cross-site scripting (XSS) vulnerability in Message Board widget in Liferay Portal 7.2.0 through 7.4.2, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 17, and older unsupported versions allows remote authenticated users to inject arbitrary web script or HTML via the filename of an attachment.	2024-02-21	9	CVE-2024-25152
liferay -- portal	Stored cross-site scripting (XSS) vulnerability in Expando module's geolocation custom fields in Liferay Portal 7.2.0 through 7.4.2, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 17, and older unsupported versions allows remote authenticated users to inject arbitrary web script or HTML via a crafted payload injected into the name text field of a geolocation custom field.	2024-02-21	9	CVE-2024-25601
liferay -- portal	Stored cross-site scripting (XSS) vulnerability in Users Admin module's edit user page in Liferay Portal 7.2.0 through 7.4.2, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 17, and older unsupported versions allows remote authenticated users to inject arbitrary web script or HTML via a crafted payload injected into an organization's "Name" text field	2024-02-21	9	CVE-2024-25602
liferay -- portal	Stored cross-site scripting (XSS) vulnerability in the Dynamic Data Mapping module's DDMForm in Liferay Portal 7.2.0 through 7.4.3.4, and older unsupported versions, and Liferay DXP 7.4.13, 7.3 before update 4, 7.2 before fix pack 17, and older unsupported versions allows remote authenticated users to inject arbitrary web script or HTML via the instanceId parameter.	2024-02-21	9	CVE-2024-25603
liferay -- portal	In Liferay Portal 7.2.0 through 7.4.3.12, and older unsupported versions, and Liferay DXP 7.4 before update 9, 7.3 before update 4, 7.2 before fix pack 19, and older unsupported versions, the default configuration does not sanitize blog entries of JavaScript, which allows remote authenticated users to inject arbitrary web script or HTML (XSS) via a crafted payload injected into a blog entry's content text field.	2024-02-20	9	CVE-2024-25610
liferay -- portal	Multiple stored cross-site scripting (XSS) vulnerabilities in Liferay Portal 7.2.0 through 7.4.3.13, and older unsupported versions, and Liferay DXP 7.4 before update 10, 7.3 before update 4, 7.2 before fix pack 17, and older unsupported versions allow remote authenticated users to inject arbitrary web script or HTML via a crafted payload injected into the first/middle/last name text field of the user who creates an entry in the (1) Announcement widget, or (2) Alerts widget.	2024-02-21	9	CVE-2024-26266
liferay -- portal	Cross-site scripting (XSS) vulnerability in the Frontend JS module's portlet.js in Liferay Portal 7.2.0 through 7.4.3.37, and Liferay DXP 7.4 before update 38, 7.3 before update 11, 7.2 before fix pack 20, and older unsupported versions allows remote attackers to inject arbitrary web script or HTML via the anchor (hash) part of a URL.	2024-02-21	9.6	CVE-2024-26269
liferay -- portal	XXE vulnerability in Liferay Portal 7.2.0 through 7.4.3.7, and older unsupported versions, and Liferay DXP 7.4 before update 4, 7.3 before update 12, 7.2 before fix	2024-02-20	8	CVE-2024-25606

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	pack 20, and older unsupported versions allows attackers with permission to deploy widgets/portlets/extensions to obtain sensitive information or consume system resources via the Java2WsddTask._format method.			
liferay -- portal	The default password hashing algorithm (PBKDF2-HMAC-SHA1) in Liferay Portal 7.2.0 through 7.4.3.15, and older unsupported versions, and Liferay DXP 7.4 before update 16, 7.3 before update 4, 7.2 before fix pack 17, and older unsupported versions defaults to a low work factor, which allows attackers to quickly crack password hashes.	2024-02-20	8.1	CVE-2024-25607
loomio -- loomio	Loomio version 2.22.0 allows executing arbitrary commands on the server. This is possible because the application is vulnerable to OS Command Injection.	2024-02-20	10	CVE-2024-1297
mantisbt -- mantisbt	MantisBT is an open source issue tracker. Prior to version 2.26.1, an unauthenticated attacker who knows a user's email address and username can hijack the user's account by poisoning the link in the password reset notification message. A patch is available in version 2.26.1. As a workaround, define `$g_path` as appropriate in `config_inc.php`.	2024-02-20	8.3	CVE-2024-23830
mastodon -- mastodon	Mastodon is a free, open-source social network server based on ActivityPub. Prior to versions 4.2.7, 4.1.15, 4.0.15, and 3.5.19, when fetching remote statuses, Mastodon doesn't check that the response from the remote server has a `Content-Type` header value of the Activity Streams media type, which allows a threat actor to upload a crafted Activity Streams document to a remote server and make a Mastodon server fetch it, if the remote server accepts arbitrary user uploads. The vulnerability allows a threat actor to impersonate an account on a remote server that satisfies all of the following properties: allows the attacker to register an account; accepts arbitrary user-uploaded documents and places them on the same domain as the ActivityPub actors; and serves user-uploaded document in response to requests with an `Accept` header value of the Activity Streams media type. Versions 4.2.7, 4.1.15, 4.0.15, and 3.5.19 contain a fix for this issue.	2024-02-19	8.5	CVE-2024-25623
materialsproject -- pymatgen	Pymatgen (Python Materials Genomics) is an open-source Python library for materials analysis. A critical security vulnerability exists in the `JonesFaithfulTransformation.from_transformation_str()` method within the `pymatgen` library prior to version 2024.2.20. This method insecurely utilizes `eval()` for processing input, enabling execution of arbitrary code when parsing untrusted input. Version 2024.2.20 fixes this issue.	2024-02-21	9.3	CVE-2024-23346
microsoft -- microsoft_edge_(chromium-based)	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	2024-02-23	8.2	CVE-2024-26192
misskey-dev -- misskey	Misskey is an open source, decentralized social media platform with ActivityPub support. Prior to version 2024.2.0, when fetching remote Activity Streams objects, Misskey doesn't check that the response from the remote server has a `Content-Type` header value of the Activity Streams media type, which allows a threat actor to upload a crafted Activity Streams document to a remote server and make a Misskey instance fetch it, if the remote server accepts arbitrary user uploads. The vulnerability allows a threat actor to impersonate and take over an account on a remote server that satisfies all of the following properties: allows the threat actor to register an account; accepts arbitrary user-uploaded documents and places them on the same domain as legitimate Activity Streams actors; and serves user-uploaded document in response to requests with an `Accept` header value of the Activity Streams media type. Version 2024.2.0 contains a patch for the issue.	2024-02-19	7.1	CVE-2024-25636
mlflow -- mflow	Insufficient sanitization in MLflow leads to XSS when running an untrusted recipe. This issue leads to a client-side RCE when running an untrusted recipe in Jupyter Notebook. The vulnerability stems from lack of sanitization over template variables.	2024-02-23	7.5	CVE-2024-27132
mlflow -- mflow	Insufficient sanitization in MLflow leads to XSS when running a recipe that uses an untrusted dataset. This issue leads to a client-side RCE when running the recipe in Jupyter Notebook. The vulnerability stems from lack of sanitization over dataset table fields.	2024-02-23	7.5	CVE-2024-27133
moodle -- moodle	Insufficient file size checks resulted in a denial of service risk in the file picker's unzip functionality.	2024-02-19	7.5	CVE-2024-25978
ni -- systemlink_server	Incorrect permissions in the installation directories for shared SystemLink Elixir based services may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-20	7.8	CVE-2024-1155

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ni -- systemlink_server	Incorrect directory permissions for the shared NI RabbitMQ service may allow a local authenticated user to read RabbitMQ configuration information and potentially enable escalation of privileges.	2024-02-20	7.8	CVE-2024-1156
onnx -- onnx	Versions of the package onnx before and including 1.15.0 are vulnerable to Directory Traversal as the external_data field of the tensor proto can have a path to the file which is outside the model current directory or user-provided directory. The vulnerability occurs as a bypass for the patch added for CVE-2022-25882.	2024-02-23	7.5	CVE-2024-27318
open_vswitch -- open_vswitch	A flaw was found in Open vSwitch where multiple versions are vulnerable to crafted Geneve packets, which may result in a denial of service and invalid memory accesses. Triggering this issue requires that hardware offloading via the netlink path is enabled.	2024-02-22	7.5	CVE-2023-3966
oppo -- usercenter_credit_sdk	In OPPO Usercenter Credit SDK, there's a possible escalation of privilege due to loose permission check, This could lead to application internal information leak w/o user interaction.	2024-02-20	9.1	CVE-2024-1608
pgjdbc -- pgjdbc	pgjdbc, the PostgreSQL JDBC Driver, allows attacker to inject SQL if using PreferQueryMode=SIMPLE. Note this is not the default. In the default mode there is no vulnerability. A placeholder for a numeric value must be immediately preceded by a minus. There must be a second placeholder for a string value after the first placeholder; both must be on the same line. By constructing a matching string payload, the attacker can inject SQL to alter the query,bypassing the protections that parameterized queries bring against SQL Injection attacks. Versions before 42.7.2, 42.6.1, 42.5.5, 42.4.4, 42.3.9, and 42.2.8 are affected.	2024-02-19	10	CVE-2024-1597
pimcore -- admin-ui-classic-bundle	Pimcore's Admin Classic Bundle provides a Backend UI for Pimcore. A potential security vulnerability has been discovered in `pimcore/admin-ui-classic-bundle` prior to version 1.3.4. The vulnerability involves a Host Header Injection in the `invitationLinkAction` function of the UserController, specifically in the way `$loginUrl` trusts user input. The host header from incoming HTTP requests is used unsafely when generating URLs. An attacker can manipulate the HTTP host header in requests to the /admin/user/invitationlink endpoint, resulting in the generation of URLs with the attacker's domain. In fact, if a host header is injected in the POST request, the $loginURL parameter is constructed with this unvalidated host header. It is then used to send an invitation email to the provided user. This vulnerability can be used to perform phishing attacks by making the URLs in the invitation links emails point to an attacker-controlled domain. Version 1.3.4 contains a patch for the vulnerability. The maintainers recommend validating the host header and ensuring it matches the application's domain. It would also be beneficial to use a default trusted host or hostname if the incoming host header is not recognized or is absent.	2024-02-19	8.1	CVE-2024-25625
powerpack_addons_for_elementor -- powerpack_pro_for_elementor	Cross-Site Request Forgery (CSRF) vulnerability in PowerPack Addons for Elementor PowerPack Pro for Elementor.This issue affects PowerPack Pro for Elementor: from n/a before 2.10.8.	2024-02-21	7.1	CVE-2024-24843
progress_software -- loadmaster	Unauthenticated remote attackers can access the system through the LoadMaster management interface, enabling arbitrary system command execution.	2024-02-21	10	CVE-2024-1212
progress_software_coproration -- ws_ftp_server	In WS_FTP Server versions before 8.8.5, reflected cross-site scripting issues have been identified on various user supplied inputs on the WS_FTP Server administrative interface.	2024-02-21	7.5	CVE-2024-1474
pyca -- cryptography	cryptography is a package designed to expose cryptographic primitives and recipes to Python developers. Starting in version 38.0.0 and prior to version 42.0.4, if `pkcs12.serialize_key_and_certificates` is called with both a certificate whose public key did not match the provided private key and an `encryption_algorithm` with `hmac_hash` set (via `PrivateFormat.PKCS12.encryption_builder().hmac_hash(...)`, then a NULL pointer dereference would occur, crashing the Python process. This has been resolved in version 42.0.4, the first version in which a `ValueError` is properly raised.	2024-02-21	7.5	CVE-2024-26130
pyhtml2pdf -- pyhtml2pdf	Pyhtml2pdf version 0.0.6 allows an external attacker to remotely obtain arbitrary local files. This is possible because the application does not validate the HTML content entered by the user.	2024-02-20	7.5	CVE-2024-1647
silicon_labs -- gecko_platform	A heap-based buffer overflow vulnerability exists in the HTTP Server functionality of WestonFF Embedded uC-HTTP git commit 80d4004. A specially crafted network packet can lead to arbitrary code execution. An attacker can send a malicious packet to trigger this vulnerability.	2024-02-20	10	CVE-2023-45318

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sitepact -- sitepact	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Sitepact.This issue affects Sitepact: from n/a through 1.0.5.	2024-02-23	7.1	CVE-2024-25928
sourcecodester -- complete_file_management_system	A vulnerability, which was classified as critical, was found in SourceCodester Complete File Management System 1.0. Affected is an unknown function of the file users/index.php of the component Login Form. The manipulation of the argument username with the input torada%27+or+%271%27+%3D+%271%27+--+- 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-254622 is the identifier assigned to this vulnerability.	2024-02-23	7.3	CVE-2024-1831
sourcecodester -- complete_file_management_system	A vulnerability has been found in SourceCodester Complete File Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/ of the component Admin Login Form. The manipulation of the argument username with the input torada%27+or+%271%27+%3D+%271%27+--+- 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-254623.	2024-02-23	7.3	CVE-2024-1832
sourcecodester -- employee_management_system	A vulnerability was found in SourceCodester Employee Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /Account/login.php. The manipulation of the argument txtusername 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-254624.	2024-02-23	7.3	CVE-2024-1833
spring -- spring_framework	Applications that use UriComponentsBuilder to parse an externally provided URL (e.g. through a query parameter) AND perform validation checks on the host of the parsed URL may be vulnerable to an open redirect https://cwe.mitre.org/data/definitions/601.html attack or to a SSRF attack if the URL is used after passing validation checks.	2024-02-23	8.1	CVE-2024-22243
spring -- spring_security	In Spring Security, versions 6.1.x prior to 6.1.7 and versions 6.2.x prior to 6.2.2, an application is vulnerable to broken access control when it directly uses the AuthenticationTrustResolver.isFullyAuthenticated(Authentication);method. Specifically, an application is vulnerable if: * The application uses AuthenticationTrustResolver.isFullyAuthenticated(Authentication) directly and a null authentication parameter is passed to it resulting in an erroneous true return value. An application is not vulnerable if any of the following is true: * The application does not use AuthenticationTrustResolver.isFullyAuthenticated(Authentication) directly. * The application does not pass null to AuthenticationTrustResolver.isFullyAuthenticated * The application only uses isFullyAuthenticated via Method Security https://docs.spring.io/spring-security/reference/servlet/authorization/method-security.html or HTTP Request Security https://docs.spring.io/spring-security/reference/servlet/authorization/authorize-http-requests.html	2024-02-20	7.4	CVE-2024-22234
suite_crm -- suite_crm	Suite CRM version 7.14.2 allows including local php files. This is possible because the application is vulnerable to LFI.	2024-02-20	9.9	CVE-2024-1644
tenable -- tenable_identity_exposure_secure_relay	A DLL injection vulnerability exists where an authenticated, low-privileged local attacker could modify application files on the TIE Secure Relay host, which could allow for overriding of the configuration and running of new Secure Relay services.	2024-02-23	7.3	CVE-2024-1683
the_biosig_project -- libbiosig	A heap-based buffer overflow vulnerability exists in the .egi parsing functionality of The Biosig Project libbiosig 2.5.0 and Master Branch (ab0ee111). A specially crafted .egi file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	2024-02-20	9.8	CVE-2024-21795
the_biosig_project -- libbiosig	A double-free vulnerability exists in the BrainVision Header Parsing functionality of The Biosig Project libbiosig Master Branch (ab0ee111) and 2.5.0. A specially crafted .vdhr file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	2024-02-20	9.8	CVE-2024-22097
the_biosig_project -- libbiosig	An integer overflow vulnerability exists in the sopen_FAMOS_read functionality of The Biosig Project libbiosig 2.5.0 and Master Branch (ab0ee111). A specially crafted .famos file can lead to an out-of-bounds write which in turn can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	2024-02-20	9.8	CVE-2024-21812
the_biosig_project -- libbiosig	An out-of-bounds write vulnerability exists in the BrainVisionMarker Parsing functionality of The Biosig Project libbiosig 2.5.0 and Master Branch (ab0ee111). A specially crafted .vmrk file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	2024-02-20	9.8	CVE-2024-23305

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
the_biosig_project -- libbiosig	A use-after-free vulnerability exists in the sopen_FAMOS_read functionality of The Biosig Project libbiosig 2.5.0 and Master Branch (ab0ee111). A specially crafted .famos file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	2024-02-20	9.8	CVE-2024-23310
the_biosig_project -- libbiosig	An integer underflow vulnerability exists in the sopen_FAMOS_read functionality of The Biosig Project libbiosig 2.5.0 and Master Branch (ab0ee111). A specially crafted .famos file can lead to an out-of-bounds write which in turn can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	2024-02-20	9.8	CVE-2024-23313
the_biosig_project -- libbiosig	An out-of-bounds write vulnerability exists in the sopen_FAMOS_read functionality of The Biosig Project libbiosig 2.5.0 and Master Branch (ab0ee111). A specially crafted .famos file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	2024-02-20	9.8	CVE-2024-23606
the_biosig_project -- libbiosig	A double-free vulnerability exists in the BrainVision ASCII Header Parsing functionality of The Biosig Project libbiosig 2.5.0 and Master Branch (ab0ee111). A specially crafted .vdhr file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	2024-02-20	9.8	CVE-2024-23809
torrentpier -- torrentpier	Torrentpier version 2.4.1 allows executing arbitrary commands on the server. This is possible because the application is vulnerable to insecure deserialization.	2024-02-20	10	CVE-2024-1651
totolink -- lr1200gb	A vulnerability classified as critical has been found in Totolink LR1200GB 9.1.0u.6619_B20230130/9.3.5u.6698_B20230810. Affected is the function loginAuth of the file /cgi-bin/cstecgi.cgi of the component Web Interface. The manipulation of the argument http_host 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-254574 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-23	9.8	CVE-2024-1783
undertow -- undertow	A vulnerability was found in Undertow. This vulnerability impacts a server that supports the wildfly-http-client protocol. Whenever a malicious user opens and closes a connection with the HTTP port of the server and then closes the connection immediately, the server will end with both memory and open file limits exhausted at some point, depending on the amount of memory available. At HTTP upgrade to remoting, the WriteTimeoutStreamSinkConduit leaks connections if RemotingConnection is closed by Remoting ServerConnectionOpenListener. Because the remoting connection originates in Undertow as part of the HTTP upgrade, there is an external layer to the remoting connection. This connection is unaware of the outermost layer when closing the connection during the connection opening procedure. Hence, the Undertow WriteTimeoutStreamSinkConduit is not notified of the closed connection in this scenario. Because WriteTimeoutStreamSinkConduit creates a timeout task, the whole dependency tree leaks via that task, which is added to XNIO WorkerThread. So, the workerThread points to the Undertow conduit, which contains the connections and causes the leak.	2024-02-19	7.5	CVE-2024-1635
veritas -- ediscovery_platform	A vulnerability was discovered in Veritas eDiscovery Platform before 10.2.5. The application administrator can upload potentially malicious files to arbitrary locations on the server on which the application is installed.	2024-02-22	7.2	CVE-2024-27283
vmware -- vmware_enhanced_authentication_plug-in_(eap)	Arbitrary Authentication Relay and Session Hijack vulnerabilities in the deprecated VMware Enhanced Authentication Plug-in (EAP) could allow a malicious actor that could trick a target domain user with EAP installed in their web browser into requesting and relaying service tickets for arbitrary Active Directory Service Principal Names (SPNs).	2024-02-20	9.6	CVE-2024-22245
vmware -- vmware_enhanced_authentication_plug-in_(eap)	Session Hijack vulnerability in Deprecated VMware Enhanced Authentication Plug-in could allow a malicious actor with unprivileged local access to a windows operating system can hijack a privileged EAP session when initiated by a privileged domain user on the same system.	2024-02-20	7.8	CVE-2024-22250
weston_embedded -- uc-tcp-ip	A double-free vulnerability exists in the IP header loopback parsing functionality of Weston Embedded uC-TCP-IP v3.06.01. A specially crafted set of network packets can lead to memory corruption, potentially resulting in code execution. An attacker can send a sequence of unauthenticated packets to trigger this vulnerability.	2024-02-20	8.7	CVE-2023-38562
ylianst -- meshcentral	MeshCentral is a full computer management web site. Versions prior to 1.1.21 a cross-site websocket hijacking (CSWSH) vulnerability within the control.ashx endpoint. This component is the primary mechanism used within MeshCentral to perform administrative actions on the server. The vulnerability is exploitable when an attacker is able to convince a victim end-user to click on a malicious link to a	2024-02-20	8.3	CVE-2024-26135

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	page hosting an attacker-controlled site. The attacker can then originate a cross-site websocket connection using client-side JavaScript code to connect to `control.ashx` as the victim user within MeshCentral. Version 1.1.21 contains a patch for this issue.			
yoctoproject -- poky	Yocto Project is an open source collaboration project that helps developers create custom Linux-based systems regardless of the hardware architecture. In Yocto Projects Bitbake before 2.6.2 (before and included Yocto Project 4.3.1), with the Toaster server (included in bitbake) running, missing input validation allows an attacker to perform a remote code execution in the server's shell via a crafted HTTP request. Authentication is not necessary. Toaster server execution has to be specifically run and is not the default for Bitbake command line builds, it is only used for the Toaster web based user interface to Bitbake. The fix has been backported to the bitbake included with Yocto Project 5.0, 3.1.31, 4.0.16, and 4.3.2.	2024-02-19	8.8	CVE-2024-25626
zephyrproject-rtos -- zephyr	Signed to unsigned conversion esp32_ipm_send	2024-02-18	8	CVE-2023-6249
zephyrproject-rtos -- zephyr	Unchecked length coming from user input in settings shell	2024-02-18	8	CVE-2023-6749
zephyrproject-rtos -- zephyr	The documentation specifies that the BT_GATT_PERM_READ_LESC and BT_GATT_PERM_WRITE_LESC defines for a Bluetooth characteristic: Attribute read/write permission with LE Secure Connection encryption. If set, requires that LE Secure Connections is used for read/write access, however this is only true when it is combined with other permissions, namely BT_GATT_PERM_READ_ENCRYPT/BT_GATT_PERM_READ_AUTHEN (for read) or BT_GATT_PERM_WRITE_ENCRYPT/BT_GATT_PERM_WRITE_AUTHEN (for write), if these additional permissions are not set (even in secure connections only mode) then the stack does not perform any permission checks on these characteristics and they can be freely written/read.	2024-02-19	8.2	CVE-2024-1638
zestardtechnologies -- admin_side_data_storage_for_contact_form_7	The Admin side data storage for Contact Form 7 plugin for WordPress is vulnerable to SQL Injection via the 'form-id' parameter in all versions up to, and including, 1.1.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-02-23	7.2	CVE-2024-1776
zyxel -- atp_series_firmware	A format string vulnerability in a function of the IPSec VPN feature in Zyxel ATP series firmware versions from 4.32 through 5.37 Patch 1, USG FLEX series firmware versions from 4.50 through 5.37 Patch 1, USG FLEX 50(W) series firmware versions from 4.16 through 5.37 Patch 1, and USG20(W)-VPN series firmware versions from 4.16 through 5.37 Patch 1 could allow an attacker to achieve unauthorized remote code execution by sending a sequence of specially crafted payloads containing an invalid pointer; however, such an attack would require detailed knowledge of an affected device's memory layout and configuration.	2024-02-20	8.1	CVE-2023-6764
zyxel -- atp_series_firmware	A post-authentication command injection vulnerability in the file upload binary in Zyxel ATP series firmware versions from 4.32 through 5.37 Patch 1, USG FLEX series firmware versions from 4.50 through 5.37 Patch 1, USG FLEX 50(W) series firmware versions from 4.16 through 5.37 Patch 1, USG20(W)-VPN series firmware versions from 4.16 through 5.37 Patch 1, USG FLEX H series firmware versions from 1.10 through 1.10 Patch 1, NWA50AX firmware versions through 6.29(ABYW.3), WAC500 firmware versions through 6.65(ABVS.1), WAX300H firmware versions through 6.60(ACHF.1), and WBE660S firmware versions through 6.65(ACGG.1) could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands on an affected device via FTP.	2024-02-20	7.2	CVE-2023-6398
9bis -- kitty	KiTTY versions 0.76.1.13 and before is vulnerable to command injection via the filename variable, occurs due to insufficient input sanitization and validation, failure to escape special characters, and insecure system calls (at lines 2369-2390). This allows an attacker to add inputs inside the filename variable, leading to arbitrary code execution.	2024-02-09	7.8	CVE-2024-23749
9bis -- kitty	KiTTY versions 0.76.1.13 and before is vulnerable to a stack-based buffer overflow via the hostname, occurs due to insufficient bounds checking and input sanitization. This allows an attacker to overwrite adjacent memory, which leads to arbitrary code execution.	2024-02-09	7.8	CVE-2024-25003

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
9bis -- kitty	KiTTY versions 0.76.1.13 and before is vulnerable to a stack-based buffer overflow via the username, occurs due to insufficient bounds checking and input sanitization (at line 2600). This allows an attacker to overwrite adjacent memory, which leads to arbitrary code execution.	2024-02-09	7.8	CVE-2024-25004
adobe -- acrobat_reader	Acrobat Reader versions 20.005.30539, 23.008.20470 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	7.8	CVE-2024-20726
adobe -- acrobat_reader	Acrobat Reader versions 20.005.30539, 23.008.20470 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	7.8	CVE-2024-20727
adobe -- acrobat_reader	Acrobat Reader versions 20.005.30539, 23.008.20470 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	7.8	CVE-2024-20728
adobe -- acrobat_reader	Acrobat Reader versions 20.005.30539, 23.008.20470 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	7.8	CVE-2024-20729
adobe -- acrobat_reader	Acrobat Reader versions 20.005.30539, 23.008.20470 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	7.8	CVE-2024-20730
adobe -- acrobat_reader	Acrobat Reader versions 20.005.30539, 23.008.20470 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	7.8	CVE-2024-20731
adobe -- adobe_framemaker	Adobe Framemaker versions 2022.1 and earlier are affected by an Improper Authentication vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass authentication mechanisms and gain unauthorized access. Exploitation of this issue does not require user interaction.	2024-02-15	9.8	CVE-2024-20738
adobe -- audition	Audition versions 24.0.3, 23.6.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	7.8	CVE-2024-20739
adobe -- commerce	Adobe Commerce versions 2.4.6-p3, 2.4.5-p5, 2.4.4-p6 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin attacker to inject malicious scripts into every admin page. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field, that could be leveraged to gain admin access.	2024-02-15	9.1	CVE-2024-20719
adobe -- commerce	Adobe Commerce versions 2.4.6-p3, 2.4.5-p5, 2.4.4-p6 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an attacker. Exploitation of this issue does not require user interaction.	2024-02-15	9.1	CVE-2024-20720
adobe -- substance3d_-_designer	Substance3D - Designer versions 13.1.0 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	7.8	CVE-2024-20750
adobe -- substance_3d_painter	Substance3D - Painter versions 9.1.1 and earlier are affected by a Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	7.8	CVE-2024-20723
adobe -- substance_3d_painter	Substance3D - Painter versions 9.1.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	7.8	CVE-2024-20740
adobe -- substance_3d_painter	Substance3D - Painter versions 9.1.1 and earlier are affected by a Write-what-where Condition vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	7.8	CVE-2024-20741

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- substance_3d_painter	Substance3D - Painter versions 9.1.1 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	7.8	CVE-2024-20742
adobe -- substance_3d_painter	Substance3D - Painter versions 9.1.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	7.8	CVE-2024-20743
adobe -- substance_3d_painter	Substance3D - Painter versions 9.1.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	7.8	CVE-2024-20744
alayacare -- procura_portal	Publicly known cryptographic machine key in AlayaCare's Procura Portal before 9.0.1.2 allows attackers to forge their own authentication cookies and bypass the application's authentication mechanisms.	2024-02-16	8.6	CVE-2023-6451
alfio-event -- alf.io	Alf.io is a free and open-source event attendance management system. In versions prior to 2.0-M4-2402 users can access the admin area even after being invalidated/deleted. This issue has been addressed in version 2.0-M4-2402. All users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-16	7.6	CVE-2024-25628
angular -- angular	This affects versions of the package angular from 1.3.0. A regular expression used to split the value of the ng-srcset directive is vulnerable to super-linear runtime due to backtracking. With a large carefully-crafted input, this can result in catastrophic backtracking and cause a denial of service. **Note:** This package is EOL and will not receive any updates to address this issue. Users should migrate to [@angular/core](https://www.npmjs.com/package/@angular/core).	2024-02-10	7.5	CVE-2024-21490
apache -- solr	Improper Control of Dynamically-Managed Code Resources, Unrestricted Upload of File with Dangerous Type, Inclusion of Functionality from Untrusted Control Sphere vulnerability in Apache Solr. This issue affects Apache Solr: from 6.0.0 through 8.11.2, from 9.0.0 before 9.4.1. In the affected versions, Solr ConfigSets accepted Java jar and class files to be uploaded through the ConfigSets API. When backing up Solr Collections, these configSet files would be saved to disk when using the LocalFileSystemRepository (the default for backups). If the backup was saved to a directory that Solr uses in its ClassPath/ClassLoaders, then the jar and class files would be available to use with any ConfigSet, trusted or untrusted. When Solr is run in a secure way (Authorization enabled), as is strongly suggested, this vulnerability is limited to extending the Backup permissions with the ability to add libraries. Users are recommended to upgrade to version 8.11.3 or 9.4.1, which fix the issue. In these versions, the following protections have been added: * Users are no longer able to upload files to a configSet that could be executed via a Java ClassLoader. * The Backup API restricts saving backups to directories that are used in the ClassLoader.	2024-02-09	8.8	CVE-2023-50386
apache -- solr	Insufficiently Protected Credentials vulnerability in Apache Solr. This issue affects Apache Solr: from 6.0.0 through 8.11.2, from 9.0.0 before 9.3.0. One of the two endpoints that publishes the Solr process' Java system properties, /admin/info/properties, was only setup to hide system properties that had "password" contained in the name. There are a number of sensitive system properties, such as "basicauth" and "aws.secretKey" do not contain "password", thus their values were published via the "/admin/info/properties" endpoint. This endpoint populates the list of System Properties on the home screen of the Solr Admin page, making the exposed credentials visible in the UI. This /admin/info/properties endpoint is protected under the "config-read" permission. Therefore, Solr Clouds with Authorization enabled will only be vulnerable through logged-in users that have the "config-read" permission. Users are recommended to upgrade to version 9.3.0 or 8.11.3, which fixes the issue. A single option now controls hiding Java system property for all endpoints, "-Dsolr.hiddenSysProps". By default all known sensitive properties are hidden (including "-Dbasicauth"), as well as any property with a name containing "secret" or "password". Users who cannot upgrade can also use the following Java system property to fix the issue: '-Dsolr.redaction.system.pattern=.*(password|secret|basicauth).*'	2024-02-09	7.5	CVE-2023-50291
apache -- solr	Incorrect Permission Assignment for Critical Resource, Improper Control of Dynamically-Managed Code Resources vulnerability in Apache Solr. This issue affects Apache Solr: from 8.10.0 through 8.11.2, from 9.0.0 before 9.3.0. The	2024-02-09	7.5	CVE-2023-50292

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Schema Designer was introduced to allow users to more easily configure and test new Schemas and configSets. However, when the feature was created, the "trust" (authentication) of these configSets was not considered. External library loading is only available to configSets that are "trusted" (created by authenticated users), thus non-authenticated users are unable to perform Remote Code Execution. Since the Schema Designer loaded configSets without taking their "trust" into account, configSets that were created by unauthenticated users were allowed to load external libraries when used in the Schema Designer. Users are recommended to upgrade to version 9.3.0, which fixes the issue.			
apache -- solr	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Solr. This issue affects Apache Solr: from 6.0.0 through 8.11.2, from 9.0.0 before 9.4.1. Solr Streaming Expressions allows users to extract data from other Solr Clouds, using a "zkHost" parameter. When original SolrCloud is setup to use ZooKeeper credentials and ACLs, they will be sent to whatever "zkHost" the user provides. An attacker could setup a server to mock ZooKeeper, that accepts ZooKeeper requests with credentials and ACLs and extracts the sensitive information, then send a streaming expression using the mock server's address in "zkHost". Streaming Expressions are exposed via the "/streaming" handler, with "read" permissions. Users are recommended to upgrade to version 8.11.3 or 9.4.1, which fix the issue. From these versions on, only zkHost values that have the same server address (regardless of chroot), will use the given ZooKeeper credentials and ACLs when connecting.	2024-02-09	7.5	CVE-2023-50298
azure -- azure-uamqp_c	The UAMQP is a general purpose C library for AMQP 1.0. During a call to open_get_offered_capabilities, a memory allocation may fail causing a use-after-free issue and if a client called it during connection communication it may cause a remote code execution. Users are advised to update the submodule with commit `30865c9c`. There are no known workarounds for this vulnerability.	2024-02-12	9.8	CVE-2024-25110
boostmyshop -- boostmyshop	SQL Injection vulnerability in Boostmyshop (boostmyshopagent) module for Prestashop versions 1.1.9 and before, allows remote attackers to escalate privileges and obtain sensitive information via changeOrderCarrier.php, relayPoint.php, and shippingConfirmation.php.	2024-02-09	9.8	CVE-2024-24308
code-projects -- cinema_seat_reservation_system	Code-projects Cinema Seat Reservation System 1.0 allows SQL Injection via the 'id' parameter at "/Cinema-Reservation/booking.php?id=1."	2024-02-09	9.8	CVE-2024-25307
code-projects -- simple_school_management_system	Code-projects Simple School Managment System 1.0 allows SQL Injection via the 'apass' parameter at "School/index.php."	2024-02-09	8.8	CVE-2024-25304
code-projects -- simple_school_management_system	Code-projects Simple School Managment System 1.0 allows Authentication Bypass via the username and password parameters at School/index.php.	2024-02-09	8.8	CVE-2024-25305
code-projects -- simple_school_management_system	Code-projects Simple School Managment System 1.0 allows SQL Injection via the 'aname' parameter at "School/index.php".	2024-02-09	8.8	CVE-2024-25306
code-projects -- simple_school_management_system	Code-projects Simple School Managment System 1.0 allows SQL Injection via the 'name' parameter at School/teacher_login.php.	2024-02-09	8.8	CVE-2024-25308
code-projects -- simple_school_management_system	Code-projects Simple School Managment System 1.0 allows SQL Injection via the 'pass' parameter at School/teacher_login.php.	2024-02-09	8.8	CVE-2024-25309
code-projects -- simple_school_management_system	Code-projects Simple School Managment System 1.0 allows SQL Injection via the 'id' parameter at "School/delete.php?id=5."	2024-02-09	8.8	CVE-2024-25310
code-projects -- simple_school_management_system	Code-projects Simple School Managment System 1.0 allows SQL Injection via the 'id' parameter at "School/sub_delete.php?id=5."	2024-02-09	8.8	CVE-2024-25312
code-projects -- simple_school_management_system	Code-projects Simple School Managment System 1.0 allows Authentication Bypass via the username and password parameters at School/teacher_login.php.	2024-02-09	8.8	CVE-2024-25313
comarch -- erp_xl	Comarch ERP XL client is vulnerable to MS SQL protocol downgrade request from a server side, what could lead to an unencrypted communication vulnerable to data interception and modification. This issue affects ERP XL: from 2020.2.2 through 2023.2.	2024-02-15	7.4	CVE-2023-4537
comarch -- erp_xl	Use of a hard-coded password for a special database account created during Comarch ERP XL installation allows an attacker to retrieve embedded sensitive data	2024-02-15	7.5	CVE-2023-4539

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	stored in the database. The password is same among all Comarch ERP XL installations. This issue affects ERP XL: from 2020.2.2 through 2023.2.			
contiki-ng -- contiki-ng	Contiki-NG is an open-source, cross-platform operating system for Next-Generation IoT devices. An attacker can trigger out-of-bounds reads in the RPL-Lite implementation of the RPL protocol in the Contiki-NG operating system. This vulnerability is caused by insufficient control of the lengths for DIO and DAO messages, in particular when they contain RPL sub-option headers. The problem has been patched in Contiki-NG 4.9. Users are advised to upgrade. Users unable to upgrade should manually apply the code changes in PR #2484.	2024-02-14	8.6	CVE-2023-50927
contiki-ng -- contiki-ng	Contiki-NG is an open-source, cross-platform operating system for Next-Generation IoT devices. An out-of-bounds write exists in the driver for IEEE 802.15.4 radios on nRF platforms in the Contiki-NG operating system. The problem is triggered when parsing radio frames in the `read_frame` function in the `arch/cpu/nrf/net/nrf-ieee-driver-arch.c` module. More specifically, the `read_frame` function performs an incomplete validation of the payload length of the packet, which is a value that can be set by an external party that sends radio packets to a Contiki-NG system. Although the value is validated to be in the range of the MTU length, it is not validated to fit into the given buffer into which the packet will be copied. The problem has been patched in the "develop" branch of Contiki-NG and is expected to be included in subsequent releases. Users are advised to update their develop branch or to update to a subsequent release when available. Users unable to upgrade should consider manually applying the changes in PR #2741.	2024-02-14	7	CVE-2023-48229
contiki-ng -- contiki-ng	Contiki-NG is an open-source, cross-platform operating system for Next-Generation IoT devices. An out-of-bounds read can be caused by an incoming DIO message when using the RPL-Lite implementation in the Contiki-NG operating system. More specifically, the prefix information of the DIO message contains a field that specifies the length of an IPv6 address prefix. The value of this field is not validated, which means that an attacker can set a value that is longer than the maximum prefix length. Subsequently, a memcmp function call that compares different prefixes can be called with a length argument that surpasses the boundary of the array allocated for the prefix, causing an out-of-bounds read. The problem has been patched in the "develop" branch of Contiki-NG, and is expected to be included in the next release. Users are advised to update as soon as they are able to or to manually apply the changes in Contiki-NG pull request #2721.	2024-02-14	7.5	CVE-2023-50926
dell -- dell_smartfabric_os10	Dell OS10 Networking Switches running 10.5.2.x and above contain a vulnerability with zeroMQ when VLT is configured. A remote unauthenticated attacker could potentially exploit this vulnerability leading to information disclosure and a possible Denial of Service when a huge number of requests are sent to the switch. This is a high severity vulnerability as it allows an attacker to view sensitive data. Dell recommends customers to upgrade at the earliest opportunity.	2024-02-15	9.1	CVE-2023-28078
dell -- dell_smartfabric_os10	Dell OS10 Networking Switches running 10.5.2.x and above contain an OS command injection vulnerability when using remote user authentication. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands and possible system takeover. This is a critical vulnerability as it allows an attacker to cause severe damage. Dell recommends customers to upgrade at the earliest opportunity.	2024-02-15	9.8	CVE-2023-32462
dell -- enterprise_sonic_os	Dell Networking Switches running Enterprise SONiC versions 4.1.0, 4.0.5, 3.5.4 and below contains an improper input validation vulnerability. A remote unauthenticated malicious user may exploit this vulnerability and escalate privileges up to the highest administrative level. This is a Critical vulnerability affecting certain protocols, Dell recommends customers to upgrade at the earliest opportunity.	2024-02-15	9.8	CVE-2023-32484
dell -- esi_(enterprise_storage_integrator)_for_sap_lama	DELL ESI (Enterprise Storage Integrator) for SAP LAMA, version 10.0, contains an information disclosure vulnerability in EHAC component. A remote unauthenticated attacker could potentially exploit this vulnerability by eavesdropping the network traffic to gain admin level credentials.	2024-02-15	9.8	CVE-2023-39245
dell -- esi_(enterprise_storage_integrator)_for_sap_lama	DELL ESI (Enterprise Storage Integrator) for SAP LAMA, version 10.0, contains an improper access control vulnerability in EHAC component. A remote unauthenticated attacker could potentially exploit this vulnerability to gain unrestricted access to the SOAP APIs.	2024-02-15	7.3	CVE-2023-39244

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dell -- powerprotect_data_manager	Dell PowerProtect Data Manager, version 19.15 and prior versions, contain a weak password recovery mechanism for forgotten passwords. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to unauthorized access to the application with privileges of the compromised account. The attacker could retrieve the reset password token without authorization and then perform the password change	2024-02-13	8.8	CVE-2024-22454
dell -- powerprotect_data_manager	Dell PowerProtect Data Manager, version 19.15 and prior versions, contain an OS command injection vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application. Exploitation may lead to a system take over by an attacker.	2024-02-13	7.2	CVE-2024-22445
dell -- recoverpoint_for_vms	Dell RecoverPoint for Virtual Machines 5.3.x contains an OS Command injection vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to execute arbitrary operating system commands, which will get executed in the context of the root user, resulting in a complete system compromise.	2024-02-16	7.2	CVE-2024-22426
dell -- supportassist_client_consumer	Dell SupportAssist for Home PCs Installer Executable file version prior to 3.13.2.19 used for initial installation has a high vulnerability that can result in local privilege escalation (LPE). This vulnerability only affects first-time installations done prior to 8th March 2023	2024-02-14	7.2	CVE-2023-25535
dell -- supportassist_for_home_pcs	In Dell SupportAssist for Home PCs (between v3.0 and v3.14.1) and SupportAssist for Business PCs (between v3.0 and v3.4.1), a security concern has been identified, impacting locally authenticated users on their respective PCs. This issue may potentially enable privilege escalation and the execution of arbitrary code, in the Windows system context, and confined to that specific local PC.	2024-02-14	7.8	CVE-2023-44283
dell -- unity_operating_environment	Dell Unity, versions prior to 5.4, contain an OS Command Injection Vulnerability in its svc_topstats utility. An authenticated attacker could potentially exploit this vulnerability, leading to the execution of arbitrary commands with elevated privileges.	2024-02-12	7.8	CVE-2024-0164
dell -- unity_operating_environment	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in its svc_acldb_dump utility. An authenticated attacker could potentially exploit this vulnerability, leading to execution of arbitrary operating system commands with root privileges.	2024-02-12	7.8	CVE-2024-0165
dell -- unity_operating_environment	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in its svc_tcpdump utility. An authenticated attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands with elevated privileges.	2024-02-12	7.8	CVE-2024-0166
dell -- unity_operating_environment	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in the svc_topstats utility. An authenticated attacker could potentially exploit this vulnerability, leading to the ability to overwrite arbitrary files on the file system with root privileges.	2024-02-12	7.8	CVE-2024-0167
dell -- unity_operating_environment	Dell Unity, versions prior to 5.4, contains a Command Injection Vulnerability in svc_oscheck utility. An authenticated attacker could potentially exploit this vulnerability, leading to the ability to inject arbitrary operating system commands. This vulnerability allows an authenticated attacker to execute commands with root privileges.	2024-02-12	7.8	CVE-2024-0168
dell -- unity_operating_environment	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in its svc_cava utility. An authenticated attacker could potentially exploit this vulnerability, escaping the restricted shell and execute arbitrary operating system commands with root privileges.	2024-02-12	7.8	CVE-2024-0170
dell -- unity_operating_environment	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability within its svc_udoctor utility. An authenticated malicious user with local access could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application.	2024-02-12	7.8	CVE-2024-22222
dell -- unity_operating_environment	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability within its svc_cbr utility. An authenticated malicious user with local access could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application.	2024-02-12	7.8	CVE-2024-22223
dell -- unity_operating_environment	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in its svc_nas utility. An authenticated attacker could potentially exploit this vulnerability, escaping the restricted shell and execute arbitrary operating system commands with root privileges.	2024-02-12	7.8	CVE-2024-22224

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dell -- unity_operating_environment	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in its svc_supportassist utility. An authenticated attacker could potentially exploit this vulnerability, leading to execution of arbitrary operating system commands with root privileges.	2024-02-12	7.8	CVE-2024-22225
dell -- unity_operating_environment	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in its svc_dc utility. An authenticated attacker could potentially exploit this vulnerability, leading to the ability execute commands with root privileges.	2024-02-12	7.8	CVE-2024-22227
dell -- unity_operating_environment	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in its svc_cifssupport utility. An authenticated attacker could potentially exploit this vulnerability, escaping the restricted shell and execute arbitrary operating system commands with root privileges.	2024-02-12	7.8	CVE-2024-22228
diracgrid -- dirac	DIRAC is a distributed resource framework. In affected versions any user could get a token that has been requested by another user/agent. This may expose resources to unintended parties. This issue has been addressed in release version 8.0.37. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-09	7.5	CVE-2024-24825
ebm_technologies -- risweb	EBM Technologies RISWEB's specific query function parameter does not properly restrict user input, and this feature page is accessible without login. This allows remote attackers to inject SQL commands without authentication, enabling them to read, modify, and delete database records.	2024-02-15	9.8	CVE-2024-26264
ebm_technologies -- uniweb/solipacs_webserver	EBM Technologies Uniweb/SoliPACS WebServer's query functionality lacks proper restrictions of user input, allowing remote attackers authenticated as regular user to inject SQL commands for reading, modifying, and deleting database records, as well as executing system commands. Attackers may even leverage the dbo privilege in the database for privilege escalation, elevating their privileges to administrator.	2024-02-15	8.8	CVE-2024-26262
ec-web -- fs-ezviewer(web)	EC-WEB FS-EZViewer (Web)'s query functionality lacks proper restrictions of user input, allowing remote attackers authenticated as regular user to inject SQL commands for reading, modifying, and deleting database records, as well as executing system commands. Attackers may even leverage the dbo privilege in the database for privilege escalation, elevating their privileges to administrator.	2024-02-15	8.8	CVE-2024-1523
emerson -- gc370xa_firmware	In Emerson Rosemount GC370XA, GC700XA, and GC1500XA products, an unauthenticated user with network access could obtain access to sensitive information or cause a denial-of-service condition.	2024-02-09	9.1	CVE-2023-43609
emerson -- gc370xa_firmware	In Emerson Rosemount GC370XA, GC700XA, and GC1500XA products, an unauthenticated user with network access could execute arbitrary commands in root context from a remote computer.	2024-02-09	9.8	CVE-2023-46687
emerson -- gc370xa_firmware	In Emerson Rosemount GC370XA, GC700XA, and GC1500XA products, an authenticated user with network access could run arbitrary commands from a remote computer.	2024-02-09	9.8	CVE-2023-49716
emerson -- gc370xa_firmware	In Emerson Rosemount GC370XA, GC700XA, and GC1500XA products, an unauthenticated user with network access could bypass authentication and acquire admin capabilities.	2024-02-09	8.1	CVE-2023-51761
enlightenment -- imlib2	An issue in the imlib_load_image_with_error_return function of imlib2 v1.9.1 allows attackers to cause a heap buffer overflow via parsing a crafted image.	2024-02-09	8.8	CVE-2024-25447
enlightenment -- imlib2	An issue in the imlib_free_image_and_decache function of imlib2 v1.9.1 allows attackers to cause a heap buffer overflow via parsing a crafted image.	2024-02-09	8.8	CVE-2024-25448
enlightenment -- imlib2	imlib2 v1.9.1 was discovered to mishandle memory allocation in the function init_imlib_fonts().	2024-02-09	8.8	CVE-2024-25450
envoyproxy -- envoy	Envoy is a high-performance edge/middle/service proxy. Envoy will crash when certain timeouts happen within the same interval. The crash occurs when the following are true: 1. hedge_on_per_try_timeout is enabled, 2. per_try_idle_timeout is enabled (it can only be done in configuration), 3. per-try-timeout is enabled, either through headers or configuration and its value is equal, or within the backoff interval of the per_try_idle_timeout. This issue has been addressed in released 1.29.1, 1.28.1, 1.27.3, and 1.26.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-09	7.5	CVE-2024-23322
envoyproxy -- envoy	Envoy is a high-performance edge/middle/service proxy. External authentication can be bypassed by downstream connections. Downstream clients can force invalid gRPC requests to be sent to ext_authz, circumventing ext_authz checks when failure_mode_allow is set to true. This issue has been addressed in released 1.29.1, 1.28.1, 1.27.3, and 1.26.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-09	7.5	CVE-2024-23324

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
envoyproxy -- envoy	Envoy is a high-performance edge/middle/service proxy. Envoy crashes in Proxy protocol when using an address type that isn't supported by the OS. Envoy is susceptible to crashing on a host with IPv6 disabled and a listener config with proxy protocol enabled when it receives a request where the client presents its IPv6 address. It is valid for a client to present its IPv6 address to a target server even though the whole chain is connected via IPv4. This issue has been addressed in released 1.29.1, 1.28.1, 1.27.3, and 1.26.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-09	7.5	CVE-2024-23325
envoyproxy -- envoy	Envoy is a high-performance edge/middle/service proxy. When PPv2 is enabled both on a listener and subsequent cluster, the Envoy instance will segfault when attempting to craft the upstream PPv2 header. This occurs when the downstream request has a command type of LOCAL and does not have the protocol block. This issue has been addressed in releases 1.29.1, 1.28.1, 1.27.3, and 1.26.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-09	7.5	CVE-2024-23327
eset_spol_s_r.o. -- eset_nod32_antivirus	Local privilege escalation vulnerability potentially allowed an attacker to misuse ESET's file operations to delete files without having proper permission.	2024-02-15	7.8	CVE-2024-0353
f5 -- big-ip	When running in appliance mode, an authenticated remote command injection vulnerability exists in an undisclosed iControl REST endpoint on multi-bladed systems. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2024-02-14	8.7	CVE-2024-22093
f5 -- big-ip	When BIG-IP AFM Device DoS or DoS profile is configured with NXDOMAIN attack vector and bad actor detection, undisclosed queries can cause the Traffic Management Microkernel (TMM) to terminate. NOTE: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2024-02-14	7.5	CVE-2024-21763
f5 -- big-ip	For unspecified traffic patterns, BIG-IP AFM IPS engine may spend an excessive amount of time matching the traffic against signatures, resulting in Traffic Management Microkernel (TMM) restarting and traffic disruption. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2024-02-14	7.5	CVE-2024-21771
f5 -- big-ip	When a BIG-IP ASM/Advanced WAF security policy is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2024-02-14	7.5	CVE-2024-21789
f5 -- big-ip	When an Advanced WAF/ASM security policy and a Websockets profile are configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-02-14	7.5	CVE-2024-21849
f5 -- big-ip	When BIG-IP is deployed in high availability (HA) and an iControl REST API token is updated, the change does not sync to the peer device. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2024-02-14	7.2	CVE-2024-22389
f5 -- big-ip	When a BIG-IP Advanced WAF or BIG-IP ASM policy with a Request Body Handling option is attached to a virtual server, undisclosed requests can cause the BD process to terminate. The condition results from setting the Request Body Handling option in the Header-Based Content Profile for an Allowed URL with "Apply value and content signatures and detect threat campaigns." Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2024-02-14	7.5	CVE-2024-23308
f5 -- big-ip	When HTTP/2 is configured on BIG-IP or BIG-IP Next SPK systems, undisclosed responses can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2024-02-14	7.5	CVE-2024-23314
f5 -- big-ip	Undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. For the Application Visibility and Reporting module, this may occur when the HTTP Analytics profile with URLs enabled under Collected Entities is configured on a virtual server and the DB variables avr.IncludeServerInURI or avr.CollectOnlyHostnameFromURI are enabled. For BIG-IP Advanced WAF and ASM, this may occur when either a DoS or Bot Defense profile is configured on a virtual server and the DB variables avr.IncludeServerInURI or avr.CollectOnlyHostnameFromURI are enabled. Note: The DB variables avr.IncludeServerInURI and avr.CollectOnlyHostnameFromURI are not enabled by default. For more information about the HTTP Analytics profile and the Collect URLs setting, refer to K30875743: Create a new Analytics profile and attach it to your virtual servers https://my.f5.com/manage/s/article/K30875743 . Note:	2024-02-14	7.5	CVE-2024-23805

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Software versions which have reached End of Technical Support (EoTS) are not evaluated			
f5 -- big-ip	When SSL Client Certificate LDAP or Certificate Revocation List Distribution Point (CRLDP) authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2024-02-14	7.5	CVE-2024-23979
f5 -- big-ip	When a BIG-IP PEM classification profile is configured on a UDP virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. This issue affects classification engines using signatures released between 09-08-2022 and 02-16-2023. See the table in the F5 Security Advisory for a complete list of affected classification signature files. NOTE: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2024-02-14	7.5	CVE-2024-23982
f5 -- nginx_plus	When NGINX Plus or NGINX OSS are configured to use the HTTP/3 QUIC module, undisclosed requests can cause NGINX worker processes to terminate. Note: The HTTP/3 QUIC module is not enabled by default and is considered experimental. For more information, refer to Support for QUIC and HTTP/3 https://nginx.org/en/docs/quic.html . NOTE: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2024-02-14	7.5	CVE-2024-24989
f5 -- nginx_plus	When NGINX Plus or NGINX OSS are configured to use the HTTP/3 QUIC module, undisclosed requests can cause NGINX worker processes to terminate. Note: The HTTP/3 QUIC module is not enabled by default and is considered experimental. For more information, refer to Support for QUIC and HTTP/3 https://nginx.org/en/docs/quic.html . Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2024-02-14	7.5	CVE-2024-24990
filseclab -- twister_antivirus	Twister Antivirus v8.17 allows Elevation of Privileges on the computer where it's installed by triggering the 0x80112067, 0x801120CB and 0x801120CC IOCTL codes of the fildds.sys driver.	2024-02-13	7.8	CVE-2024-1096
flusity -- flusity	flusity-CMS v2.33 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /core/tools/add_translation.php.	2024-02-11	8.8	CVE-2024-25417
flusity -- flusity	flusity-CMS v2.33 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /core/tools/delete_menu.php.	2024-02-11	8.8	CVE-2024-25418
flusity -- flusity	flusity-CMS v2.33 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /core/tools/update_menu.php.	2024-02-11	8.8	CVE-2024-25419
fortinet -- forticlientems	An improper privilege management vulnerability [CWE-269] in Fortinet FortiClientEMS version 7.2.0 through 7.2.2 and before 7.0.10 allows a Site administrator with Super Admin privileges to perform global administrative operations affecting other sites via crafted HTTP or HTTPS requests.	2024-02-15	8.8	CVE-2023-45581
fortinet -- fortiproxy	A out-of-bounds write in Fortinet FortiOS versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, 6.0.0 through 6.0.17, FortiProxy versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7 allows attacker to execute unauthorized code or commands via specifically crafted requests	2024-02-09	9.8	CVE-2024-21762
fortinet -- fortiswitchmanager	A use of externally-controlled format string in Fortinet FortiOS versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13, FortiProxy versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14, FortiPAM versions 1.2.0, 1.1.0 through 1.1.2, 1.0.0 through 1.0.3, FortiSwitchManager versions 7.2.0 through 7.2.3, 7.0.0 through 7.0.3 allows attacker to execute unauthorized code or commands via specially crafted packets.	2024-02-15	9.8	CVE-2024-23113
g5theme -- ere_recently_viewed_essential_real_estate_add-on	Deserialization of Untrusted Data vulnerability in G5Theme ERE Recently Viewed - Essential Real Estate Add-On. This issue affects ERE Recently Viewed - Essential Real Estate Add-On: from n/a through 1.3.	2024-02-12	9.8	CVE-2024-24797
gambio -- gambio	Deserialization of Untrusted Data in Gambio through 4.9.2.0 allows attackers to run arbitrary code via "search" parameter of the Parcelshopfinder/AddAddressBookEntry" function.	2024-02-12	9.8	CVE-2024-23759
gambio -- gambio	Server Side Template Injection in Gambio 4.9.2.0 allows attackers to run arbitrary code via crafted smarty email template.	2024-02-12	9.8	CVE-2024-23761
gambio -- gambio	SQL Injection vulnerability in Gambio through 4.9.2.0 allows attackers to run arbitrary SQL commands via crafted GET request using modifiers[attribute][] parameter.	2024-02-12	9.8	CVE-2024-23763
gambio -- gambio	Unrestricted File Upload vulnerability in Content Manager feature in Gambio 4.9.2.0 allows attackers to execute arbitrary code via upload of crafted PHP file.	2024-02-12	7.8	CVE-2024-23762

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
getcomposer -- composer	Composer is a dependency Manager for the PHP language. In affected versions several files within the local working directory are included during the invocation of Composer and in the context of the executing user. As such, under certain conditions arbitrary code execution may lead to local privilege escalation, provide lateral user movement or malicious code execution when Composer is invoked within a directory with tampered files. All Composer CLI commands are affected, including composer.phar's self-update. The following scenarios are of high risk: Composer being run with sudo, Pipelines which may execute Composer on untrusted projects, Shared environments with developers who run Composer individually on the same project. This vulnerability has been addressed in versions 2.7.0 and 2.2.23. It is advised that the patched versions are applied at the earliest convenience. Where not possible, the following should be addressed: Remove all sudo composer privileges for all users to mitigate root privilege escalation, and avoid running Composer within an untrusted directory, or if needed, verify that the contents of `vendor/composer/InstalledVersions.php` and `vendor/composer/installed.php` do not include untrusted code. A reset can also be done on these files by the following:```sh rm vendor/composer/installed.php vendor/composer/InstalledVersions.php composer install --no-scripts --no-plugins ```	2024-02-09	7.8	CVE-2024-24821
github -- enterprise_server	A command injection vulnerability was identified in GitHub Enterprise Server that allowed an attacker with an editor role in the Management Console to gain admin SSH access to the appliance via the actions-console docker container while setting a service URL. Exploitation of this vulnerability required access to the GitHub Enterprise Server instance and access to the Management Console with the editor role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.11.5, 3.10.7, 3.9.10, and 3.8.15. This vulnerability was reported via the GitHub Bug Bounty program.	2024-02-13	9.1	CVE-2024-1355
github -- enterprise_server	A command injection vulnerability was identified in GitHub Enterprise Server that allowed an attacker with an editor role in the Management Console to gain admin SSH access to the appliance when setting up an HTTP proxy. Exploitation of this vulnerability required access to the GitHub Enterprise Server instance and access to the Management Console with the editor role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.11.5, 3.10.7, 3.9.10, and 3.8.15. This vulnerability was reported via the GitHub Bug Bounty program https://bounty.github.com.	2024-02-13	9.1	CVE-2024-1359
github -- enterprise_server	A command injection vulnerability was identified in GitHub Enterprise Server that allowed an attacker with an editor role in the Management Console to gain admin SSH access to the appliance when setting the username and password for collected configurations. Exploitation of this vulnerability required access to the GitHub Enterprise Server instance and access to the Management Console with the editor role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.11.5, 3.10.7, 3.9.10, and 3.8.15. This vulnerability was reported via the GitHub Bug Bounty program https://bounty.github.com.	2024-02-13	9.1	CVE-2024-1369
github -- enterprise_server	A command injection vulnerability was identified in GitHub Enterprise Server that allowed an attacker with an editor role in the Management Console to gain admin SSH access to the appliance when configuring SAML settings. Exploitation of this vulnerability required access to the GitHub Enterprise Server instance and access to the Management Console with the editor role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.11.5, 3.10.7, 3.9.10, and 3.8.15. This vulnerability was reported via the GitHub Bug Bounty program https://bounty.github.com.	2024-02-13	9.1	CVE-2024-1372
github -- enterprise_server	A command injection vulnerability was identified in GitHub Enterprise Server that allowed an attacker with an editor role in the Management Console to gain admin SSH access to the appliance via nomad templates when configuring audit log forwarding. Exploitation of this vulnerability required access to the GitHub Enterprise Server instance and access to the Management Console with the editor role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.11.5, 3.10.7, 3.9.10, and 3.8.15. This vulnerability was reported via the GitHub Bug Bounty program https://bounty.github.com.	2024-02-13	9.1	CVE-2024-1374
github -- enterprise_server	A command injection vulnerability was identified in GitHub Enterprise Server that allowed an attacker with an editor role in the Management Console to gain admin SSH access to the appliance via nomad templates when configuring SMTP options. Exploitation of this vulnerability required access to the GitHub Enterprise Server	2024-02-13	9.1	CVE-2024-1378

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	instance and access to the Management Console with the editor role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.11.5, 3.10.7, 3.9.10, and 3.8.15. This vulnerability was reported via the GitHub Bug Bounty program https://bounty.github.com.			
github -- enterprise_server	A command injection vulnerability was identified in GitHub Enterprise Server that allowed an attacker with an editor role in the Management Console to gain admin SSH access to the appliance via the `syslog-ng` configuration file. Exploitation of this vulnerability required access to the GitHub Enterprise Server instance and access to the Management Console with the editor role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.11.5, 3.10.7, 3.9.10, and 3.8.15. This vulnerability was reported via the GitHub Bug Bounty program.	2024-02-13	8	CVE-2024-1354
github -- enterprise_server	An incorrect authorization vulnerability was identified in GitHub Enterprise Server that allowed an attacker to create new branches in public repositories and run arbitrary GitHub Actions workflows with permissions from the GITHUB_TOKEN. To exploit this vulnerability, an attacker would need access to the Enterprise Server. This vulnerability affected all versions of GitHub Enterprise Server after 3.8 and prior to 3.12, and was fixed in versions 3.9.10, 3.10.7, 3.11.5. This vulnerability was reported via the GitHub Bug Bounty program.	2024-02-14	7.1	CVE-2024-1482
grafana -- grafana_son_datasource	The JSON data source plugin (https://grafana.com/grafana/plugins/marcusolsson-json-datasource/ https://grafana.com/grafana/plugins/marcusolsson-json-datasource/) is a Grafana Labs maintained plugin for Grafana that allows for retrieving and processing JSON data from a remote endpoint (including a specific sub-path) configured by an administrator. Due to inadequate sanitization of the dashboard-supplied path parameter, it was possible to include path traversal characters (../) in the path parameter and send requests to paths on the configured endpoint outside the configured sub-path. This means that if the data source was configured by an administrator to point at some sub-path of a domain (e.g. https://example.com/api/some_safe_api/ https://example.com/api/some_safe_api/), it was possible for an editor to create a dashboard referencing the data source which issues queries containing path traversal characters, which would in turn cause the data source to instead query arbitrary subpaths on the configured domain (e.g. https://example.com/api/admin_api/) https://example.com/api/admin_api/) . In the rare case that this plugin is configured by an administrator to point back at the Grafana instance itself, this vulnerability becomes considerably more severe, as an administrator browsing a maliciously configured panel could be compelled to make requests to Grafana administrative API endpoints with their credentials, resulting in the potential for privilege escalation, hence the high score for this vulnerability.	2024-02-14	8	CVE-2023-5123
hcltech -- sametime	Sametime is impacted by a Cross Site Request Forgery (CSRF) vulnerability. Some REST APIs in the Sametime Proxy application can allow an attacker to perform malicious actions on the application.	2024-02-09	8.8	CVE-2023-50349
hgiga -- oaklouds	The functionality for synchronization in HGiga OAKlouds' certain modules has an OS Command Injection vulnerability, allowing remote attackers to inject system commands within specific request parameters. This enables the execution of arbitrary code on the remote server without permission.	2024-02-15	9.8	CVE-2024-26260
hgiga -- oaklouds	The functionality for file download in HGiga OAKlouds' certain modules contains an Arbitrary File Read and Delete vulnerability. Attackers can put file path in specific request parameters, allowing them to download the file without login. Furthermore, the file will be deleted after being downloaded.	2024-02-15	9.8	CVE-2024-26261
hima -- f30_03x_yy_(com)	An unauthenticated remote attacker can use an uncontrolled resource consumption vulnerability to DoS the affected devices through excessive traffic on a single ethernet port.	2024-02-13	7.5	CVE-2024-24781
hotel_management_system_project -- hotel_management_system	Code-projects Hotel Managment System 1.0, allows SQL Injection via the 'sid' parameter in Hotel/admin/show.php?sid=2.	2024-02-09	9.8	CVE-2024-25314
hotel_management_system_project -- hotel_management_system	Code-projects Hotel Managment System 1.0, allows SQL Injection via the 'rid' parameter in Hotel/admin/roombook.php?rid=2.	2024-02-09	9.8	CVE-2024-25315

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hotel_management_system_project -- hotel_management_system	Code-projects Hotel Managment System 1.0 allows SQL Injection via the 'eid' parameter in Hotel/admin/usersettingdel.php?eid=2.	2024-02-09	9.8	CVE-2024-25316
hotel_management_system_project -- hotel_management_system	Code-projects Hotel Managment System 1.0 allows SQL Injection via the 'pid' parameter in Hotel/admin/print.php?pid=2.	2024-02-09	8.8	CVE-2024-25318
hugin_project -- hugin	An issue in the HuginBase::PanoramaMemento::loadPTScript function of Hugin v2022.0.0 allows attackers to cause a heap buffer overflow via parsing a crafted image.	2024-02-09	7.8	CVE-2024-25442
hugin_project -- hugin	An issue in the HuginBase::ImageVariable<double>::linkWith function of Hugin v2022.0.0 allows attackers to cause a heap-use-after-free via parsing a crafted image.	2024-02-09	7.8	CVE-2024-25443
hugin_project -- hugin	Improper handling of values in HuginBase::PTools::Transform::transform of Hugin 2022.0.0 leads to an assertion failure.	2024-02-09	7.8	CVE-2024-25445
hugin_project -- hugin	An issue in the HuginBase::PTools::setDestImage function of Hugin v2022.0.0 allows attackers to cause a heap buffer overflow via parsing a crafted image.	2024-02-09	7.8	CVE-2024-25446
ibm -- engineering_lifecycle_optimization	IBM Engineering Lifecycle Optimization - Publishing 7.0.2 and 7.0.3 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 268749.	2024-02-09	8.8	CVE-2023-45187
ibm -- engineering_lifecycle_optimization	IBM Engineering Lifecycle Optimization 7.0.2 and 7.0.3 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 268755.	2024-02-09	7.5	CVE-2023-45191
ibm -- semeru_runtime	IBM Semeru Runtime 8.0.302.0 through 8.0.392.0, 11.0.12.0 through 11.0.21.0, 17.0.1.0 - 17.0.9.0, and 21.0.1.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 281222.	2024-02-10	7.5	CVE-2024-22361
ibm -- storage_defender_resiliency_service	IBM Storage Defender - Resiliency Service 2.0 could allow a privileged user to perform unauthorized actions after obtaining encrypted data from clear text key storage. IBM X-Force ID: 275783.	2024-02-10	7.2	CVE-2023-50957
ibm -- storage_defender_resiliency_service	IBM Storage Defender - Resiliency Service 2.0 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: 278749.	2024-02-10	7.8	CVE-2024-22313
ibm -- storage_scale_container_native_storage_access	IBM Storage Scale Container Native Storage Access 5.1.2.1 through 5.1.7.0 could allow a local attacker to initiate connections from a container outside the current namespace. IBM X-Force ID: 237811.	2024-02-17	7.1	CVE-2022-41737
ibm -- storage_scale_container_native_storage_access	IBM Storage Scale Container Native Storage Access 5.1.2.1 -through 5.1.7.0 could allow an attacker to initiate connections to containers from external networks. IBM X-Force ID: 237812.	2024-02-17	7.5	CVE-2022-41738
icinga -- icinga	Icinga Director is a tool designed to make Icinga 2 configuration handling easy. Not any of Icinga Director's configuration forms used to manipulate the monitoring environment are protected against cross site request forgery (CSRF). It enables attackers to perform changes in the monitoring environment managed by Icinga Director without the awareness of the victim. Users of the map module in version 1.x, should immediately upgrade to v2.0. The mentioned XSS vulnerabilities in Icinga Web are already fixed as well and upgrades to the most recent release of the 2.9, 2.10 or 2.11 branch must be performed if not done yet. Any later major release is also suitable. Icinga Director will receive minor updates to the 1.8, 1.9, 1.10 and 1.11 branches to remedy this issue. Upgrade immediately to a patched release. If that is not feasible, disable the director module for the time being.	2024-02-09	8.3	CVE-2024-24820
icinga -- icingaweb2-module-incubator	icingaweb2-module-incubator is a working project of bleeding edge Icinga Web 2 libraries. In affected versions the class `gipfl\Web\Form` is the base for various concrete form implementations [1] and provides protection against cross site request forgery (CSRF) by default. This is done by automatically adding an element with a CSRF token to any form, unless explicitly disabled, but even if enabled, the CSRF token (sent during a client's submission of a form relying on it) is not	2024-02-09	8.8	CVE-2024-24819

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	validated. This enables attackers to perform changes on behalf of a user which, unknowingly, interacts with a prepared link or website. The version 0.22.0 is available to remedy this issue. Users are advised to upgrade. There are no known workarounds for this vulnerability.			
innovadeluxe -- manufacturer_or_supplier_alphabetical_search	SQL injection vulnerability in InnovaDeluxe "Manufacturer or supplier alphabetical search" (idxrmanufacturer) module for PrestaShop versions 2.0.4 and before, allows remote attackers to escalate privileges and obtain sensitive information via the methods IdxrmanufacturerFunctions::getCornersLink, IdxrmanufacturerFunctions::getManufacturersLike and IdxrmanufacturerFunctions::getSuppliersLike.	2024-02-09	9.8	CVE-2023-46350
intel -- intel(r)_dsa_software	Improper access control in some Intel(R) DSA software before version 23.4.33 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	8.8	CVE-2023-39425
intel -- intel(r)_oneapi_dpc++/c++_compiler_software	Improper access control in some Intel(R) oneAPI DPC++/C++ Compiler software before version 2023.2.1 may allow authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	7.8	CVE-2023-35121
intel -- intel(r)_pcm_software	Buffer underflow in some Intel(R) PCM software before version 202307 may allow an unauthenticated user to potentially enable denial of service via network access.	2024-02-14	7.5	CVE-2023-34351
intel -- intel(r)_proset/wireless_and_intel(r)_killer(tm)_wi	Improper access control for some Intel(R) PROSet/Wireless and Intel(R) Killer(TM) Wi-Fi software before version 22.240 may allow an unauthenticated user to potentially enable denial of service via local access.	2024-02-14	7.1	CVE-2023-33875
intel -- intel(r)_sur_software	Improper access control in some Intel(R) SUR software before version 2.4.10587 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	2024-02-14	7.1	CVE-2023-39941
intel -- intel(r)_thunderbolt(tm)_dch_drivers_for_windows	Improper access control in the Intel(R) Thunderbolt (TM) DCH drivers for Windows may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	8.2	CVE-2023-22293
intel -- intel(r)_thunderbolt(tm)_dch_drivers_for_windows	Improper input validation in some Intel(R) Thunderbolt (TM) DCH drivers for Windows before version 88 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	7.7	CVE-2023-22342
intel -- intel(r)_thunderbolt(tm)_dch_drivers_for_windows	Improper access control in some Intel(R) Thunderbolt (TM) DCH drivers for Windows before version 88 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	7.9	CVE-2023-25777
isc -- bind_9	The DNS message parsing code in `named` includes a section whose computational complexity is overly high. It does not cause problems for typical DNS traffic, but crafted queries and responses may cause excessive CPU load on the affected `named` instance by exploiting this flaw. This issue affects both authoritative servers and recursive resolvers. This issue affects BIND 9 versions 9.0.0 through 9.16.45, 9.18.0 through 9.18.21, 9.19.0 through 9.19.19, 9.9.3-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.45-S1, and 9.18.11-S1 through 9.18.21-S1.	2024-02-13	7.5	CVE-2023-4408
isc -- bind_9	A flaw in query-handling code can cause `named` to exit prematurely with an assertion failure when: - `nxdomain-redirect <domain>;` is configured, and - the resolver receives a PTR query for an RFC 1918 address that would normally result in an authoritative NXDOMAIN response. This issue affects BIND 9 versions 9.12.0 through 9.16.45, 9.18.0 through 9.18.21, 9.19.0 through 9.19.19, 9.16.8-S1 through 9.16.45-S1, and 9.18.11-S1 through 9.18.21-S1.	2024-02-13	7.5	CVE-2023-5517
isc -- bind_9	A bad interaction between DNS64 and serve-stale may cause `named` to crash with an assertion failure during recursive resolution, when both of these features are enabled. This issue affects BIND 9 versions 9.16.12 through 9.16.45, 9.18.0 through	2024-02-13	7.5	CVE-2023-5679

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	9.18.21, 9.19.0 through 9.19.19, 9.16.12-S1 through 9.16.45-S1, and 9.18.11-S1 through 9.18.21-S1.			
isc -- bind_9	To keep its cache database efficient, `named` running as a recursive resolver occasionally attempts to clean up the database. It uses several methods, including some that are asynchronous: a small chunk of memory pointing to the cache element that can be cleaned up is first allocated and then queued for later processing. It was discovered that if the resolver is continuously processing query patterns triggering this type of cache-database maintenance, `named` may not be able to handle the cleanup events in a timely manner. This in turn enables the list of queued cleanup events to grow infinitely large over time, allowing the configured `max-cache-size` limit to be significantly exceeded. This issue affects BIND 9 versions 9.16.0 through 9.16.45 and 9.16.8-S1 through 9.16.45-S1.	2024-02-13	7.5	CVE-2023-6516
ivanti -- connect_secure	An XML external entity or XXE vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x), Ivanti Policy Secure (9.x, 22.x) and ZTA gateways which allows an attacker to access certain restricted resources without authentication.	2024-02-13	8.3	CVE-2024-22024
linksys -- wrt54gl_firmware	A vulnerability was found in Linksys WRT54GL 4.30.18 and classified as problematic. Affected by this issue is some unknown functionality of the file /SysInfo.htm of the component Web Management Interface. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-253328. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-09	7.5	CVE-2024-1404
litespeedtech -- lsquic	In LiteSpeed QUIC (LSQUIC) Library before 4.0.4, DCID validation is mishandled.	2024-02-09	9.8	CVE-2024-25678
manageengine -- exchange_reporter_plus	Zoho ManageEngine Exchange Reporter Plus versions 5714 and below are vulnerable to the Authenticated SQL injection in report exporting feature.	2024-02-16	8.3	CVE-2024-21775
mhenrixon -- sidekiq-unique-jobs	sidekiq-unique-jobs is an open-source project which prevents simultaneous Sidekiq jobs with the same unique arguments to run. Specially crafted GET request parameters handled by any of the following endpoints of sidekiq-unique-jobs' "admin" web UI, allow a super-user attacker, or an unwitting, but authorized, victim, who has received a disguised / crafted link, to successfully execute malicious code, which could potentially steal cookies, session data, or local storage data from the app the sidekiq-unique-jobs web UI is mounted in. 1. `/changelogs`, 2. `/locks` or 3. `/expiring_locks`. This issue has been addressed in versions 7.1.33 and 8.0.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-13	7.1	CVE-2024-25122
microsoft -- .net_6.0	.NET Denial of Service Vulnerability	2024-02-13	7.5	CVE-2024-21404
microsoft -- asp.net_core_6.0	.NET Denial of Service Vulnerability	2024-02-13	7.5	CVE-2024-21386
microsoft -- azure_connected_machine_agent	Azure Connected Machine Agent Elevation of Privilege Vulnerability	2024-02-13	7.3	CVE-2024-21329
microsoft -- azure_devops_server_2022	Azure DevOps Server Remote Code Execution Vulnerability	2024-02-13	7.5	CVE-2024-20667
microsoft -- azure_kubernetes_service	Microsoft Azure Kubernetes Service Confidential Container Remote Code Execution Vulnerability	2024-02-13	9	CVE-2024-21376
microsoft -- azure_kubernetes_service	Microsoft Azure Kubernetes Service Confidential Container Elevation of Privilege Vulnerability	2024-02-13	9	CVE-2024-21403
microsoft -- azure_site_recovery	Microsoft Azure Site Recovery Elevation of Privilege Vulnerability	2024-02-13	9.3	CVE-2024-21364

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- entra	Microsoft Entra Jira Single-Sign-On Plugin Elevation of Privilege Vulnerability	2024-02-13	9.8	CVE-2024-21401
microsoft -- microsoft_365_apps_for_enterprise	Microsoft Office OneNote Remote Code Execution Vulnerability	2024-02-13	7.8	CVE-2024-21384
microsoft -- microsoft_365_apps_for_enterprise	Microsoft Outlook Elevation of Privilege Vulnerability	2024-02-13	7.1	CVE-2024-21402
microsoft -- microsoft_defender_for_endpoint_for_windows	Microsoft Defender for Endpoint Protection Elevation of Privilege Vulnerability	2024-02-13	7.8	CVE-2024-21315
microsoft -- microsoft_dynamics_365_(on-premises)_version_9.1	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	2024-02-13	8.2	CVE-2024-21395
microsoft -- microsoft_dynamics_365_(on-premises)_version_9.1	Dynamics 365 Sales Spoofing Vulnerability	2024-02-13	7.6	CVE-2024-21328
microsoft -- microsoft_dynamics_365_(on-premises)_version_9.1	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	2024-02-13	7.6	CVE-2024-21389
microsoft -- microsoft_dynamics_365_(on-premises)_version_9.1	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	2024-02-13	7.6	CVE-2024-21393
microsoft -- microsoft_dynamics_365_(on-premises)_version_9.1	Dynamics 365 Field Service Spoofing Vulnerability	2024-02-13	7.6	CVE-2024-21394
microsoft -- microsoft_dynamics_365_(on-premises)_version_9.1	Dynamics 365 Sales Spoofing Vulnerability	2024-02-13	7.6	CVE-2024-21396
microsoft -- microsoft_dynamics_365_business_central_2022_release_wave_2	Microsoft Dynamics Business Central/NAV Information Disclosure Vulnerability	2024-02-13	8	CVE-2024-21380
microsoft -- microsoft_dynamics_365_customer_engagement_v9.1	Microsoft Dynamics 365 Customer Engagement Cross-Site Scripting Vulnerability	2024-02-13	7.6	CVE-2024-21327
microsoft -- microsoft_exchang	Microsoft Exchange Server Elevation of Privilege Vulnerability	2024-02-13	9.8	CVE-2024-21410

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
e_server_2016_cumulative_update_23				
microsoft -- microsoft_office_2019	Microsoft Outlook Remote Code Execution Vulnerability	2024-02-13	9.8	CVE-2024-21413
microsoft -- microsoft_office_2019	Microsoft Outlook Remote Code Execution Vulnerability	2024-02-13	8	CVE-2024-21378
microsoft -- microsoft_office_2019	Microsoft Office Remote Code Execution Vulnerability	2024-02-13	7.8	CVE-2024-20673
microsoft -- microsoft_office_2019	Microsoft Word Remote Code Execution Vulnerability	2024-02-13	7.8	CVE-2024-21379
microsoft -- windows_10_version_1809	Microsoft ActiveX Data Objects Remote Code Execution Vulnerability	2024-02-13	8.8	CVE-2024-21349
microsoft -- windows_10_version_1809	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-02-13	8.8	CVE-2024-21350
microsoft -- windows_10_version_1809	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-02-13	8.8	CVE-2024-21352
microsoft -- windows_10_version_1809	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	2024-02-13	8.1	CVE-2024-21357
microsoft -- windows_10_version_1809	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-02-13	8.8	CVE-2024-21358
microsoft -- windows_10_version_1809	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-02-13	8.8	CVE-2024-21359
microsoft -- windows_10_version_1809	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-02-13	8.8	CVE-2024-21360
microsoft -- windows_10_version_1809	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-02-13	8.8	CVE-2024-21361
microsoft -- windows_10_version_1809	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-02-13	8.8	CVE-2024-21365
microsoft -- windows_10_version_1809	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-02-13	8.8	CVE-2024-21366
microsoft -- windows_10_version_1809	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-02-13	8.8	CVE-2024-21367

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10_version_1809	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-02-13	8.8	CVE-2024-21368
microsoft -- windows_10_version_1809	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-02-13	8.8	CVE-2024-21369
microsoft -- windows_10_version_1809	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-02-13	8.8	CVE-2024-21370
microsoft -- windows_10_version_1809	Windows OLE Remote Code Execution Vulnerability	2024-02-13	8.8	CVE-2024-21372
microsoft -- windows_10_version_1809	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-02-13	8.8	CVE-2024-21375
microsoft -- windows_10_version_1809	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-02-13	8.8	CVE-2024-21391
microsoft -- windows_10_version_1809	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-02-13	8.8	CVE-2024-21420
microsoft -- windows_10_version_1809	Windows Kernel Elevation of Privilege Vulnerability	2024-02-13	7.8	CVE-2024-21338
microsoft -- windows_10_version_1809	Microsoft ODBC Driver Remote Code Execution Vulnerability	2024-02-13	7.5	CVE-2024-21347
microsoft -- windows_10_version_1809	Internet Connection Sharing (ICS) Denial of Service Vulnerability	2024-02-13	7.5	CVE-2024-21348
microsoft -- windows_10_version_1809	Microsoft Message Queuing (MSMQ) Elevation of Privilege Vulnerability	2024-02-13	7.8	CVE-2024-21354
microsoft -- windows_10_version_1809	Microsoft Message Queuing (MSMQ) Elevation of Privilege Vulnerability	2024-02-13	7	CVE-2024-21355
microsoft -- windows_10_version_1809	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	2024-02-13	7.8	CVE-2024-21363
microsoft -- windows_10_version_1809	Windows Kernel Elevation of Privilege Vulnerability	2024-02-13	7	CVE-2024-21371
microsoft -- windows_10_version_1809	Windows DNS Information Disclosure Vulnerability	2024-02-13	7.1	CVE-2024-21377
microsoft -- windows_10_version_1809	Microsoft Message Queuing (MSMQ) Elevation of Privilege Vulnerability	2024-02-13	7	CVE-2024-21405

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10_version_1809	Windows Printing Service Spoofing Vulnerability	2024-02-13	7.5	CVE-2024-21406
microsoft -- windows_11_version_21h2	Internet Shortcut Files Security Feature Bypass Vulnerability	2024-02-13	8.1	CVE-2024-21412
microsoft -- windows_11_version_21h2	Win32k Elevation of Privilege Vulnerability	2024-02-13	7.8	CVE-2024-21346
microsoft -- windows_11_version_22h2	Windows DNS Client Denial of Service Vulnerability	2024-02-13	7.5	CVE-2024-21342
microsoft -- windows_11_version_23h2	Windows SmartScreen Security Feature Bypass Vulnerability	2024-02-13	7.6	CVE-2024-21351
microsoft -- windows_server_2022_23h2_edition_(server_core_installation)	Windows Kernel Elevation of Privilege Vulnerability	2024-02-13	8.8	CVE-2024-21345
microsoft -- windows_server_2022_23h2_edition_(server_core_installation)	Microsoft WDAC ODBC Driver Remote Code Execution Vulnerability	2024-02-13	8.8	CVE-2024-21353
minbrowser -- min	In Min before 1.31.0, local files are not correctly treated as unique security origins, which allows them to improperly request cross-origin resources. For example, a local file may request other local files through an XML document.	2024-02-09	8.8	CVE-2024-25677
misp -- misp	An issue was discovered in MISP before 2.4.184. Organization logo upload is insecure because of a lack of checks for the file extension and MIME type.	2024-02-09	9.8	CVE-2024-25674
misp -- misp	An issue was discovered in MISP before 2.4.184. A client does not need to use POST to start an export generation process. This is related to app/Controller/JobsController.php and app/View/Events/export.ctp.	2024-02-09	9.8	CVE-2024-25675
nlnet_labs -- unbound	A vulnerability was found in Unbound due to incorrect default permissions, allowing any process outside the unbound group to modify the unbound runtime configuration. If a process can connect over localhost to port 8953, it can alter the configuration of unbound.service. This flaw allows an unprivileged attacker to manipulate a running instance, potentially altering forwarders, allowing them to track all queries forwarded by the local resolver, and, in some cases, disrupting resolving altogether.	2024-02-15	8	CVE-2024-1488
objectcomputing -- micronaut	Micronaut Framework is a modern, JVM-based, full stack Java framework designed for building modular, easily testable JVM applications with support for Java, Kotlin and the Groovy language. Enabled but unsecured management endpoints are susceptible to drive-by localhost attacks. While not typical of a production application, these attacks may have more impact on a development environment where such endpoints may be flipped on without much thought. A malicious/compromised website can make HTTP requests to `localhost`. Normally, such requests would trigger a CORS preflight check which would prevent the request; however, some requests are "simple" and do not require a preflight check. These endpoints, if enabled and not secured, are vulnerable to being triggered. Production environments typically disable unused endpoints and secure/restrict access to needed endpoints. A more likely victim is the developer in their local development host, who has enabled endpoints without security for the sake of easing development. This issue has been addressed in version 3.8.3. Users are advised to upgrade.	2024-02-09	7.8	CVE-2024-23639
objectcomputing -- opendds	In OpenDDS through 3.27, there is a segmentation fault for a DataWriter with a large value of resource_limits.max_samples. NOTE: the vendor's position is that	2024-02-11	7.5	CVE-2023-52427

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the product is not designed to handle a max_samples value that is too large for the amount of memory on the system.			
oduyo -- online_collection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Oduyo Financial Technology Online Collection allows SQL Injection. This issue affects Online Collection: before v.1.0.2.	2024-02-09	9.8	CVE-2023-6677
open-mss -- mss	MSS (Mission Support System) is an open-source package designed for planning atmospheric research flights. In file: `index.py`, there is a method that is vulnerable to path manipulation attack. By modifying file paths, an attacker can acquire sensitive information from different resources. The `filename` variable is joined with other variables to form a file path in `_file`. However, `filename` is a route parameter that can capture path type values i.e. values including slashes (\). So, it is possible for an attacker to manipulate the file being read by assigning a value containing ../ to `filename` and so the attacker may be able to gain access to other files on the host filesystem. This issue has been addressed in MSS version 8.3.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-15	7.3	CVE-2024-25123
open-xchange_gmbh -- ox_app_suite	CWE-522: Insufficiently Protected Credentials vulnerability exists that could cause unauthorized access to the project file in EcoStruxure Control Expert when a local user tampers with the memory of the engineering workstation.	2024-02-14	7.1	CVE-2023-27975
open-xchange_gmbh -- ox_app_suite	Processing of CID references at E-Mail can be abused to inject malicious script code that passes the sanitization engine. Malicious script code could be injected to a user's sessions when interacting with E-Mails. Please deploy the provided updates and patch releases. CID handing has been improved and resulting content is checked for malicious content. No publicly available exploits are known.	2024-02-12	7.1	CVE-2023-41704
openidc -- mod_auth_openidc	mod_auth_openidc is an OpenID Certified™ authentication and authorization module for the Apache 2.x HTTP server that implements the OpenID Connect Relying Party functionality. In affected versions missing input validation on mod_auth_openidc_session_chunks cookie value makes the server vulnerable to a denial of service (DoS) attack. An internal security audit has been conducted and the reviewers found that if they manipulated the value of the mod_auth_openidc_session_chunks cookie to a very large integer, like 99999999, the server struggles with the request for a long time and finally gets back with a 500 error. Making a few requests of this kind caused our server to become unresponsive. Attackers can craft requests that would make the server work very hard (and possibly become unresponsive) and/or crash with minimal effort. This issue has been addressed in version 2.4.15.2. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-13	7.5	CVE-2024-24814
openrefine -- openrefine	OpenRefine is a free, open-source power tool for working with messy data and improving it. A jdbc attack vulnerability exists in OpenRefine(version<=3.7.7) where an attacker may construct a JDBC query which may read files on the host filesystem. Due to the newer MySQL driver library in the latest version of OpenRefine (8.0.30), there is no associated deserialization utilization point, so original code execution cannot be achieved, but attackers can use this vulnerability to read sensitive files on the target server. This issue has been addressed in version 3.7.8. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-12	7.5	CVE-2024-23833
opentext -- alm_octane	Improper Neutralization vulnerability affects OpenText ALM Octane version 16.2.100 and above. The vulnerability could result in a remote code execution attack.	2024-02-15	7.5	CVE-2023-6123
opentext -- operations_agent	Local privilege escalation vulnerability affects OpenText Operations Agent product versions 12.15 and 12.20-12.25 when installed on no-Windows platforms. The vulnerability could allow local privilege escalation.	2024-02-15	8.8	CVE-2024-0622
oracle_corporation -- agile_plm_framework	Vulnerability in the Oracle Agile PLM product of Oracle Supply Chain (component: Export). The supported version that is affected is 9.3.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks of this vulnerability can result in takeover of Oracle Agile PLM. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2024-02-17	8.8	CVE-2024-20953
oracle_corporation -- agile_product_lifecycle_management	Vulnerability in the Oracle Agile Product Lifecycle Management for Process product of Oracle Supply Chain (component: Installation). Supported versions that are affected are Prior to 6.2.4.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile Product	2024-02-17	7.3	CVE-2024-20956

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
_for_process	Lifecycle Management for Process. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Agile Product Lifecycle Management for Process accessible data as well as unauthorized read access to a subset of Oracle Agile Product Lifecycle Management for Process accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Agile Product Lifecycle Management for Process. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/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. Easily exploitable vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Oracle Audit Vault and Database Firewall. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Audit Vault and Database Firewall accessible data. 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).	2024-02-17	7.5	CVE-2024-20909
oracle_corporation -- enterprise_manager_base_platform	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Log Management). The supported version that is affected is 13.5.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Manager Base Platform. Successful attacks require human interaction from a person other than the attacker and 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 access to critical data or complete access to all Oracle Enterprise Manager Base Platform accessible data as well as unauthorized update, insert or delete access to some of Oracle Enterprise Manager Base Platform accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:L/A:L).	2024-02-17	7.5	CVE-2024-20917
oracle_corporation -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. While the vulnerability is in Oracle WebLogic Server, 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 WebLogic Server accessible data. CVSS 3.1 Base Score 8.6 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N).	2024-02-17	8.6	CVE-2024-20927
oracle_corporation -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2024-02-17	7.5	CVE-2024-20931
phpems -- phpems	A vulnerability, which was classified as critical, has been found in PHPEMS up to 1.0. Affected by this issue is the function index of the file app/weixin/controller/index.api.php. The manipulation of the argument picurl leads to deserialization. The exploit has been disclosed to the public and may be used. VDB-253226 is the identifier assigned to this vulnerability.	2024-02-09	9.8	CVE-2024-1353
pixelfed -- pixelfed	Pixelfed is an open-source photo sharing platform. When processing requests authorization was improperly and insufficiently checked, allowing attackers to access far more functionality than users intended, including to the administrative and moderator functionality of the Pixelfed server. This vulnerability affects every version of Pixelfed between v0.10.4 and v0.11.9, inclusive. A proof of concept of this vulnerability exists. This vulnerability affects every local user of a Pixelfed server and can potentially affect the servers' ability to federate. Some user interaction is required to setup the conditions to be able to exercise the vulnerability, but the attacker could conduct this attack time-delayed manner, where user interaction is not actively required. This vulnerability has been addressed in version 0.11.11. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-12	9.9	CVE-2024-25108

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
postahsl_ -- online_payment_system	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in POSTAHSL Online Payment System allows SQL Injection. This issue affects Online Payment System: before 14.02.2024.	2024-02-15	9.8	CVE-2023-7081
presta_monster -- multi_accessories_pro	SQL injection vulnerability in Presta Monster "Multi Accessories Pro" (hsmultiaccessoriespro) module for PrestaShop versions 5.1.1 and before, allows remote attackers to escalate privileges and obtain sensitive information via the method HsAccessoriesGroupProductAbstract::getAccessoriesByIdProducts().	2024-02-09	9.8	CVE-2023-50026
propertyhive -- propertyhive	Deserialization of Untrusted Data vulnerability in PropertyHive. This issue affects PropertyHive: from n/a through 2.0.5.	2024-02-12	8.7	CVE-2024-23513
rems -- event_student_attendance_system	Sourcecodester Event Student Attendance System 1.0, allows SQL Injection via the 'student' parameter.	2024-02-09	9.8	CVE-2024-25302
rockwell_automation -- factorytalk_service_platform	A privilege escalation vulnerability exists in Rockwell Automation FactoryTalk® Service Platform (FTSP). If exploited, a malicious user with basic user group privileges could potentially sign into the software and receive FTSP Administrator Group privileges. A threat actor could potentially read and modify sensitive data, delete data and render the FTSP system unavailable.	2024-02-16	9	CVE-2024-21915
sap_se -- sap_aba_(application_basis)	In SAP ABA (Application Basis) - versions 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75I, an attacker authenticated as a user with a remote execution authorization can use a vulnerable interface. This allows the attacker to use the interface to invoke an application function to perform actions which they would not normally be permitted to perform. Depending on the function executed, the attack can read or modify any user/business data and can make the entire system unavailable.	2024-02-13	9.1	CVE-2024-22131
sap_se -- sap_cloud_connector	Due to improper validation of certificate in SAP Cloud Connector - version 2.0, attacker can impersonate the genuine servers to interact with SCC breaking the mutual authentication. Hence, the attacker can intercept the request to view/modify sensitive information. There is no impact on the availability of the system.	2024-02-13	7.4	CVE-2024-25642
sap_se -- sap_crm_webclient_ui	Print preview option in SAP CRM WebClient UI - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, S4FND 108, WEBCUIF 700, WEBCUIF 701, WEBCUIF 730, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting vulnerability. An attacker with low privileges can cause limited impact to confidentiality and integrity of the application data after successful exploitation.	2024-02-13	7.6	CVE-2024-22130
sap_se -- sap_ides_systems	SAP IDES ECC-systems contain code that permits the execution of arbitrary program code of user's choice. An attacker can therefore control the behavior of the system by executing malicious code which can potentially escalate privileges with low impact on confidentiality, integrity and availability of the system.	2024-02-13	7.4	CVE-2024-22132
sap_se -- sap_netweaver_as_java_(guided_procedures)	SAP NetWeaver AS Java (CAF - Guided Procedures) - version 7.50, allows an unauthenticated attacker to submit a malicious request with a crafted XML file over the network, which when parsed will enable him to access sensitive files and data but not modify them. There are expansion limits in place so that availability is not affected.	2024-02-13	8.6	CVE-2024-24743
sap_se -- sap_netweaver_as_java_(user_admin_application)	The User Admin application of SAP NetWeaver AS for Java - version 7.50, insufficiently validates and improperly encodes the incoming URL parameters before including them into the redirect URL. This results in Cross-Site Scripting (XSS) vulnerability, leading to a high impact on confidentiality and mild impact on integrity and availability.	2024-02-13	8.8	CVE-2024-22126
schneider_electric -- ecostruxure_control_expert	CWE-798: Use of Hard-coded Credentials vulnerability exists that could cause unauthorized access to a project file protected with application password when opening the file with EcoStruxure Control Expert.	2024-02-14	7.7	CVE-2023-6409
schneider_electric -- harmony_control_relay_rmnf22tb30	CWE-287: Improper Authentication vulnerability exists that could cause unauthorized tampering of device configuration over NFC communication.	2024-02-14	8.8	CVE-2024-0568
schneider_electric --	CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel vulnerability exists that could cause a denial of service	2024-02-14	8.1	CVE-2023-6408

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
modicon_m340_cpu_(part_numbers_bmxp34*)	and loss of confidentiality, integrity of controllers when conducting a Man in the Middle attack.			
sherlock -- employee_management_system	An issue in Employee Managment System v1.0 allows attackers to bypass authentication via injecting a crafted payload into the E-mail and Password parameters at /alogin.html.	2024-02-14	9.8	CVE-2024-25214
sherlock -- employee_management_system	Employee Managment System v1.0 was discovered to contain a SQL injection vulnerability via the pwd parameter at /aprocess.php.	2024-02-14	9.8	CVE-2024-25215
sherlock -- employee_management_system	Employee Managment System v1.0 was discovered to contain a SQL injection vulnerability via the mailud parameter at /aprocess.php.	2024-02-14	9.8	CVE-2024-25216
sherlock -- employee_management_system	Employee Managment System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /delete.php.	2024-02-14	7.2	CVE-2024-25212
sherlock -- employee_management_system	Employee Managment System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /edit.php.	2024-02-14	7.2	CVE-2024-25213
siemens -- location_intelligence_perpetual_large	A vulnerability has been identified in Location Intelligence Perpetual Large (9DE5110-8CA13-1AX0) (All versions < V4.3), Location Intelligence Perpetual Medium (9DE5110-8CA12-1AX0) (All versions < V4.3), Location Intelligence Perpetual Non-Prod (9DE5110-8CA10-1AX0) (All versions < V4.3), Location Intelligence Perpetual Small (9DE5110-8CA11-1AX0) (All versions < V4.3), Location Intelligence SUS Large (9DE5110-8CA13-1BX0) (All versions < V4.3), Location Intelligence SUS Medium (9DE5110-8CA12-1BX0) (All versions < V4.3), Location Intelligence SUS Non-Prod (9DE5110-8CA10-1BX0) (All versions < V4.3), Location Intelligence SUS Small (9DE5110-8CA11-1BX0) (All versions < V4.3). Affected products use a hard-coded secret value for the computation of a Keyed-Hash Message Authentication Code. This could allow an unauthenticated remote attacker to gain full administrative access to the application.	2024-02-13	9.8	CVE-2024-23816
siemens -- parasolid_v35.0	A vulnerability has been identified in Parasolid V35.0 (All versions < V35.0.263), Parasolid V35.1 (All versions < V35.1.252), Parasolid V36.0 (All versions < V36.0.198). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted files containing XT format. This could allow an attacker to execute code in the context of the current process.	2024-02-13	7.8	CVE-2023-49125
siemens -- polarion_alm	A vulnerability has been identified in Polarion ALM (All versions). The REST API endpoints of doorsconnector of the affected product lacks proper authentication. An unauthenticated attacker could access the endpoints, and potentially execute code.	2024-02-13	7.3	CVE-2024-23813
siemens -- polarion_alm	A vulnerability has been identified in Polarion ALM (All versions). The affected product is vulnerable due to weak file and folder permissions in the installation path. An attacker with local access could exploit this vulnerability to escalate privileges to NT AUTHORITY\SYSTEM.	2024-02-13	7.8	CVE-2023-50236
siemens -- simatic_cp_343-1	A vulnerability has been identified in SIMATIC CP 343-1 (6GK7343-1EX30-0XE0) (All versions), SIMATIC CP 343-1 Lean (6GK7343-1CX10-0XE0) (All versions), SIPLUS NET CP 343-1 (6AG1343-1EX30-7XE0) (All versions), SIPLUS NET CP 343-1 Lean (6AG1343-1CX10-2XE0) (All versions). Affected products incorrectly validate TCP sequence numbers. This could allow an unauthenticated remote attacker to create a denial-of-service condition by injecting spoofed TCP RST packets.	2024-02-13	7.5	CVE-2023-51440
siemens -- simcenter_femap	A vulnerability has been identified in Simcenter Femap (All versions < V2401.0000). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted Catia MODEL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21710)	2024-02-13	7.8	CVE-2024-24920
siemens -- simcenter_femap	A vulnerability has been identified in Simcenter Femap (All versions < V2401.0000). The affected application is vulnerable to memory corruption while parsing specially crafted Catia MODEL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21712)	2024-02-13	7.8	CVE-2024-24921
siemens -- simcenter_femap	A vulnerability has been identified in Simcenter Femap (All versions < V2401.0000). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted Catia MODEL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21715)	2024-02-13	7.8	CVE-2024-24922

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- simcenter_femap	A vulnerability has been identified in Simcenter Femap (All versions < V2401.0000), Simcenter Femap (All versions < V2306.0001). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted Catia MODEL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-22055)	2024-02-13	7.8	CVE-2024-24923
siemens -- simcenter_femap	A vulnerability has been identified in Simcenter Femap (All versions < V2306.0000). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted Catia MODEL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-22059)	2024-02-13	7.8	CVE-2024-24924
siemens -- simcenter_femap	A vulnerability has been identified in Simcenter Femap (All versions < V2306.0000). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted Catia MODEL files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-22060)	2024-02-13	7.8	CVE-2024-24925
siemens -- sinec_nms	A vulnerability has been identified in SINEC NMS (All versions < V2.0 SP1). The affected application is vulnerable to SQL injection. This could allow an unauthenticated remote attacker to execute arbitrary SQL queries on the server database.	2024-02-13	8.8	CVE-2024-23810
siemens -- sinec_nms	A vulnerability has been identified in SINEC NMS (All versions < V2.0 SP1). The affected application allows users to upload arbitrary files via TFTP. This could allow an attacker to upload malicious firmware images or other files, that could potentially lead to remote code execution.	2024-02-13	8.8	CVE-2024-23811
siemens -- sinec_nms	A vulnerability has been identified in SINEC NMS (All versions < V2.0 SP1). The affected application incorrectly neutralizes special elements when creating a report which could lead to command injection.	2024-02-13	8	CVE-2024-23812
siemens -- tecnomatix_plant_simulation	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0012), Tecnomatix Plant Simulation V2302 (All versions < V2302.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process.	2024-02-13	7.8	CVE-2024-23795
siemens -- tecnomatix_plant_simulation	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0012), Tecnomatix Plant Simulation V2302 (All versions < V2302.0006). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	2024-02-13	7.8	CVE-2024-23796
siemens -- tecnomatix_plant_simulation	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0012), Tecnomatix Plant Simulation V2302 (All versions < V2302.0006). The affected applications contain a stack overflow vulnerability while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	2024-02-13	7.8	CVE-2024-23797
siemens -- tecnomatix_plant_simulation	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0012), Tecnomatix Plant Simulation V2302 (All versions < V2302.0006). The affected applications contain a stack overflow vulnerability while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	2024-02-13	7.8	CVE-2024-23798
siemens -- tecnomatix_plant_simulation	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0012), Tecnomatix Plant Simulation V2302 (All versions < V2302.0006). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process.	2024-02-13	7.8	CVE-2024-23802
siemens -- tecnomatix_plant_simulation	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions), Tecnomatix Plant Simulation V2302 (All versions < V2302.0007). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process.	2024-02-13	7.8	CVE-2024-23803
siemens -- tecnomatix_plant_simulation	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0012), Tecnomatix Plant Simulation V2302 (All versions < V2302.0006). The affected applications contain a stack overflow vulnerability while parsing specially crafted PSOBJ files. This could allow an attacker to execute code in the context of the current process.	2024-02-13	7.8	CVE-2024-23804
siemens -- unicam_fx	A vulnerability has been identified in Unicam FX (All versions). The windows installer agent used in affected product contains incorrect use of privileged APIs that trigger the Windows Console Host (conhost.exe) as a child process with SYSTEM privileges. This could be exploited by an attacker to perform a local privilege escalation attack.	2024-02-13	7.8	CVE-2024-22042

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
simgesel -- hearing_tracking_system	Authorization Bypass Through User-Controlled Key vulnerability in Software Engineering Consultancy Machine Equipment Limited Company Hearing Tracking System allows Authentication Abuse. This issue affects Hearing Tracking System: before for IOS 7.0, for Android Latest release 1.0.	2024-02-09	8.8	CVE-2023-6724
solarwinds -- access_rights_manager	The SolarWinds Access Rights Manager was found to be susceptible to a Remote Code Execution Vulnerability. If exploited, this vulnerability allows an authenticated user to abuse a SolarWinds service resulting in remote code execution.	2024-02-15	9	CVE-2023-40057
solarwinds -- access_rights_manager	The SolarWinds Access Rights Manager (ARM) was found to be susceptible to a Directory Traversal Remote Code Execution Vulnerability. If exploited, this vulnerability allows an unauthenticated user to achieve the Remote Code Execution.	2024-02-15	9.6	CVE-2024-23476
solarwinds -- access_rights_manager	SolarWinds Access Rights Manager (ARM) was found to be susceptible to a Directory Traversal Remote Code Execution Vulnerability. If exploited, this vulnerability allows an unauthenticated user to achieve a Remote Code Execution.	2024-02-15	9.6	CVE-2024-23479
solarwinds -- access_rights_manager	SolarWinds Access Rights Manager (ARM) was found to be susceptible to a Remote Code Execution Vulnerability. If exploited, this vulnerability allows an authenticated user to abuse a SolarWinds service, resulting in remote code execution.	2024-02-15	8	CVE-2024-23478
solarwinds -- access_rights_manager	The SolarWinds Access Rights Manager (ARM) was found to be susceptible to a Directory Traversal Remote Code Execution Vulnerability. If exploited, this vulnerability allows an unauthenticated user to achieve a Remote Code Execution.	2024-02-15	7.9	CVE-2024-23477
task_manager_in_php_with_source_code_project -- task_manager_in_php_with_source_code	Task Manager App v1.0 was discovered to contain a SQL injection vulnerability via the taskID parameter at /TaskManager/EditTask.php.	2024-02-14	9.8	CVE-2024-25220
task_manager_in_php_with_source_code_project -- task_manager_in_php_with_source_code	Task Manager App v1.0 was discovered to contain a SQL injection vulnerability via the projectID parameter at /TaskManager/EditProject.php.	2024-02-14	9.8	CVE-2024-25222
tenable -- security_center	A command injection vulnerability exists where an authenticated, remote attacker with administrator privileges on the Security Center application could modify Logging parameters, which could lead to the execution of arbitrary code on the Security Center host.	2024-02-14	7.2	CVE-2024-1367
typo3 -- typo3	TYPO3 is an open source PHP based web content management system released under the GNU GPL. In affected versions of TYPO3 entities of the File Abstraction Layer (FAL) could be persisted directly via `DataHandler`. This allowed attackers to reference files in the fallback storage directly and retrieve their file names and contents. The fallback storage ("zero-storage") is used as a backward compatibility layer for files located outside properly configured file storages and within the public web root directory. Exploiting this vulnerability requires a valid backend user account. Users are advised to update to TYPO3 version 8.7.57 ELTS, 9.5.46 ELTS, 10.4.43 ELTS, 11.5.35 LTS, 12.4.11 LTS, or 13.0.1 which fix the problem described. When persisting entities of the File Abstraction Layer directly via DataHandler, `sys_file` entities are now denied by default, and `sys_file_reference` & `sys_file_metadata` entities are not permitted to reference files in the fallback storage anymore. When importing data from secure origins, this must be explicitly enabled in the corresponding DataHandler instance by using `$dataHandler->isImporting = true;`.	2024-02-13	7.1	CVE-2024-25121
uni-pa_university_marketing_&_computer_internet_trade_inc -- university_information_system	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in UNI-PA University Marketing & Computer Internet Trade Inc. University Information System allows SQL Injection. This issue affects University Information System: before 12.12.2023.	2024-02-14	9.8	CVE-2023-6441

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
utarit_information_technologies -- solipay_mobile_app	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Utarit Information Technologies SoliPay Mobile App allows SQL Injection. This issue affects SoliPay Mobile App: before 5.0.8.	2024-02-15	9.8	CVE-2023-5155
utarit_information_technologies -- solipay_mobile_app	Improper Privilege Management vulnerability in Utarit Information Technologies SoliPay Mobile App allows Collect Data as Provided by Users. This issue affects SoliPay Mobile App: before 5.0.8.	2024-02-15	7.5	CVE-2023-4993
utarit_information_technologies -- solipay_mobile_app	Use of Hard-coded Credentials vulnerability in Utarit Information Technologies SoliPay Mobile App allows Read Sensitive Strings Within an Executable. This issue affects SoliPay Mobile App: before 5.0.8.	2024-02-15	7.5	CVE-2023-6255
vercel -- pkg	pkg is tool design to bundle Node.js projects into an executables. Any native code packages built by `pkg` are written to a hardcoded directory. On unix systems, this is `/tmp/pkg/*` which is a shared directory for all users on the same local system. There is no uniqueness to the package names within this directory, they are predictable. An attacker who has access to the same local system has the ability to replace the genuine executables in the shared directory with malicious executables of the same name. A user may then run the malicious executable without realizing it has been modified. This package is deprecated. Therefore, there will not be a patch provided for this vulnerability. To check if your executable build by pkg depends on native code and is vulnerable, run the executable and check if `/tmp/pkg/` was created. Users should transition to actively maintained alternatives. We would recommend investigating Node.js 21's support for single executable applications. Given the decision to deprecate the pkg package, there are no official workarounds or remediations provided by our team. Users should prioritize migrating to other packages that offer similar functionality with enhanced security.	2024-02-09	7.8	CVE-2024-24828
wordpress -- wordpress	The Awesome Support - WordPress HelpDesk & Support Plugin plugin for WordPress is vulnerable to union-based SQL Injection via the 'q' parameter of the wpas_get_users action in all versions up to, and including, 6.1.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-02-10	8.8	CVE-2024-0594
wordpress -- wordpress	The Backuply - Backup, Restore, Migrate and Clone plugin for WordPress is vulnerable to Denial of Service in all versions up to, and including, 1.2.5. This is due to direct access of the backuply/restore_ins.php file and. This makes it possible for unauthenticated attackers to make excessive requests that result in the server running out of resources.	2024-02-09	7.5	CVE-2024-0842
wordpress -- wordpress	The Piraeus Bank WooCommerce Payment Gateway plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'MerchantReference' parameter in all versions up to, and including, 1.6.5.1 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.	2024-02-17	9.8	CVE-2024-0610
wordpress -- wordpress	The MasterStudy LMS WordPress Plugin - for Online Courses and Education plugin for WordPress is vulnerable to union based SQL Injection via the 'user' parameter of the /lms/stm-lms/order/items REST route in all versions up to, and including, 3.2.5 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.	2024-02-17	9.8	CVE-2024-1512
wordpress -- wordpress	Deserialization of Untrusted Data vulnerability in MagePeople Team Event Manager and Tickets Selling Plugin for WooCommerce - WpEvently - WordPress Plugin. This issue affects Event Manager and Tickets Selling Plugin for WooCommerce - WpEvently - WordPress Plugin: from n/a through 4.1.1.	2024-02-12	8.2	CVE-2024-24796

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Deserialization of Untrusted Data vulnerability in UnitedThemes Brooklyn | Creative Multi-Purpose Responsive WordPress Theme. This issue affects Brooklyn | Creative Multi-Purpose Responsive WordPress Theme: from n/a through 4.9.7.6.	2024-02-12	7.5	CVE-2024-24926
wp_swings -- coupon_referral_program	Deserialization of Untrusted Data vulnerability in WP Swings Coupon Referral Program. This issue affects Coupon Referral Program: from n/a through 1.7.2.	2024-02-12	10	CVE-2024-25100
wpxpo -- productx_woocommerce_builder_&_gutenberg_woocommerce_blocks	Deserialization of Untrusted Data vulnerability in wpxpo ProductX - WooCommerce Builder & Gutenberg WooCommerce Blocks. This issue affects ProductX - WooCommerce Builder & Gutenberg WooCommerce Blocks: from n/a through 3.1.4.	2024-02-12	8.7	CVE-2024-23512
x.org -- x.org	An out-of-bounds memory access flaw was found in the X.Org server. This issue can be triggered when a device frozen by a sync grab is reattached to a different master device. This issue may lead to an application crash, local privilege escalation (if the server runs with extended privileges), or remote code execution in SSH X11 forwarding environments.	2024-02-09	7.8	CVE-2024-0229
zoom_video_communications,_inc -- zoom_desktop_client_for_windows,_zoom_vdi_client_for_windows_and_zoom_meeting_sdk_for_windows	Improper input validation in Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom Meeting SDK for Windows may allow an unauthenticated user to conduct an escalation of privilege via network access.	2024-02-14	9.6	CVE-2024-24691
zoom_video_communications_inc -- zoom_clients	Untrusted search path in some Zoom 32 bit Windows clients may allow an authenticated user to conduct an escalation of privilege via local access.	2024-02-14	7.2	CVE-2024-24697
f5 -- big-ip	When a virtual server is enabled with VLAN group and SNAT listener is configured, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2024-02-14	7.5	CVE-2024-24775
allegro_ai -- clearml	Lack of authentication in all versions of the fileserver component of Allegro AI's ClearML platform allows a remote attacker to arbitrarily access, create, modify and delete files.	2024-02-06	9.8	CVE-2024-24592
allegro_ai -- clearml	A cross-site request forgery (CSRF) vulnerability in all versions of the api and web server components of Allegro AI's ClearML platform allows a remote attacker to impersonate a user by sending API requests via maliciously crafted html. Exploitation of the vulnerability allows an attacker to compromise confidential workspaces and files, leak sensitive information, and target instances of the ClearML platform within closed off networks.	2024-02-06	9.6	CVE-2024-24593
allegro_ai -- clearml	A cross-site scripting (XSS) vulnerability in all versions of the web server component of Allegro AI's ClearML platform allows a remote attacker to execute a JavaScript payload when a user views the Debug Samples tab in the web UI.	2024-02-06	9.9	CVE-2024-24594
allegro_ai -- clearml	Deserialization of untrusted data can occur in version 0.17.0 or newer of Allegro AI's ClearML platform, enabling a maliciously uploaded artifact to run arbitrary code on an end user's system when interacted with.	2024-02-06	8	CVE-2024-24590
allegro_ai -- clearml	A path traversal vulnerability in version 1.4.0 or newer of Allegro AI's ClearML platform enables a maliciously uploaded dataset to write local or remote files to an arbitrary location on an end user's system when interacted with.	2024-02-06	8	CVE-2024-24591
ampps -- ampps	A vulnerability has been found in AMPPS 2.7 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Encryption Passphrase 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.	2024-02-02	7.5	CVE-2024-1189

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Upgrading to version 4.0 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-252679. NOTE: The vendor explains that AMPPS 4.0 is a complete overhaul and the code was re-written.			
angular -- angular	This affects versions of the package angular from 1.3.0. A regular expression used to split the value of the ng-srcset directive is vulnerable to super-linear runtime due to backtracking. With a large carefully-crafted input, this can result in catastrophic backtracking and cause a denial of service. **Note:** This package is EOL and will not receive any updates to address this issue. Users should migrate to [@angular/core](https://www.npmjs.com/package/@angular/core).	2024-02-10	7.5	CVE-2024-21490
apache_software_foundation -- pulsar	Observable timing discrepancy vulnerability in Apache Pulsar SASL Authentication Provider can allow an attacker to forge a SASL Role Token that will pass signature verification. Users are recommended to upgrade to version 2.11.3, 3.0.2, or 3.1.1 which fixes the issue. Users should also consider updating the configured secret in the `saslJaasServerRoleTokenSignerSecretPath` file. Any component matching an above version running the SASL Authentication Provider is affected. That includes the Pulsar Broker, Proxy, Websocket Proxy, or Function Worker. 2.11 Pulsar users should upgrade to at least 2.11.3. 3.0 Pulsar users should upgrade to at least 3.0.2. 3.1 Pulsar users should upgrade to at least 3.1.1. Any users running Pulsar 2.8, 2.9, 2.10, and earlier should upgrade to one of the above patched versions. For additional details on this attack vector, please refer to https://codahale.com/a-lesson-in-timing-attacks/ .	2024-02-07	7.4	CVE-2023-51437
apache_software_foundation -- sling_servlets_resolver	Malicious code execution via path traversal in Apache Software Foundation Apache Sling Servlets Resolver.This issue affects all version of Apache Sling Servlets Resolver before 2.11.0. However, whether a system is vulnerable to this attack depends on the exact configuration of the system. If the system is vulnerable, a user with write access to the repository might be able to trick the Sling Servlet Resolver to load a previously uploaded script. Users are recommended to upgrade to version 2.11.0, which fixes this issue. It is recommended to upgrade, regardless of whether your system configuration currently allows this attack or not.	2024-02-06	8.5	CVE-2024-23673
apachefriends -- xampp	A buffer overflow vulnerability has been found in XAMPP affecting version 8.2.4 and earlier. An attacker could execute arbitrary code through a long file debug argument that controls the Structured Exception Handler (SEH).	2024-02-02	9.8	CVE-2024-0338
artifex -- mupdf	mupdf v1.23.9 was discovered to contain a memory leak via the menuEntry variable in the glutAddSubMenu function.	2024-02-05	7.5	CVE-2024-24258
artifex -- mupdf	mupdf v1.23.9 was discovered to contain a memory leak via the menuEntry variable in the glutAddMenuEntry function.	2024-02-05	7.5	CVE-2024-24259
automattic_inc -- crowdsignal_dashboard_polls,_surveys_&_more	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Automattic, Inc. Crowdsignal Dashboard - Polls, Surveys & more allows Reflected XSS.This issue affects Crowdsignal Dashboard - Polls, Surveys & more: from n/a through 3.0.11.	2024-02-10	7.1	CVE-2023-51488
b&r_industrial_automation -- automation_runtime	Use of a Broken or Risky Cryptographic Algorithm vulnerability in B&R Industrial Automation Automation Runtime (SDM modules). The FTP server used on the B&R Automation Runtime supports unsecure encryption mechanisms, such as SSLv3, TLSv1.0 and TLS1.1. A network-based attacker can exploit the flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected product clients. This issue affects Automation Runtime: from 14.0 before 14.93.	2024-02-05	9.8	CVE-2024-0323
b&r_industrial_automation -- automation_studio	Incorrect Permission Assignment for Critical Resource vulnerability in B&R Industrial Automation Automation Studio allows Privilege Escalation.This issue affects Automation Studio: from 4.6.0 through 4.6.X, from 4.7.0 before 4.7.7 SP, from 4.8.0 before 4.8.6 SP, from 4.9.0 before 4.9.4 SP.	2024-02-02	8.8	CVE-2020-24681
b&r_industrial_automation -- automation_studio	Unquoted Search Path or Element vulnerability in B&R Industrial Automation Automation Studio, B&R Industrial Automation NET/PVI allows Target Programs with Elevated Privileges.This issue affects Automation Studio: from 4.0 through 4.6, from 4.7.0 before 4.7.7 SP, from 4.8.0 before 4.8.6 SP, from 4.9.0 before 4.9.4 SP; NET/PVI: from 4.0 through 4.6, from 4.7.0 before 4.7.7, from 4.8.0 before 4.8.6, from 4.9.0 before 4.9.4.	2024-02-02	7.8	CVE-2020-24682
b&r_industrial_automation -- automation_studio	: Relative Path Traversal vulnerability in B&R Industrial Automation Automation Studio allows Relative Path Traversal.This issue affects Automation Studio: from 4.0 through 4.12.	2024-02-02	7.5	CVE-2021-22281
b&r_industrial_automation -- automation_studio	Improper Control of Generation of Code ('Code Injection') vulnerability in B&R Industrial Automation Automation Studio allows Local Execution of Code.This issue affects Automation Studio: from 4.0 through 4.12.	2024-02-02	7.8	CVE-2021-22282

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
biteship -- biteship_plugin_ongkos_kirim_kurir_instant_reguler_kargo	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Biteship Biteship: Plugin Ongkos Kirim Kurir Instant, Reguler, Kargo allows Reflected XSS.This issue affects Biteship: Plugin Ongkos Kirim Kurir Instant, Reguler, Kargo: from n/a through 2.2.24.	2024-02-05	7.1	CVE-2024-24866
blurams -- lumi_security_camera_a31c_firmware	An issue in Blurams Lumi Security Camera (A31C) v23.0406.435.4120 allows attackers to execute arbitrary code.	2024-02-02	9.8	CVE-2023-50488
canon_inc -- satera_lbp670c_series	Buffer overflow in WSD probe request process of Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code.*: Satera LBP670C Series/Satera MF750C Series firmware v03.07 and earlier sold in Japan. Color imageCLASS LBP674C/Color imageCLASS X LBP1333C/Color imageCLASS MF750C Series/Color imageCLASS X MF1333C Series firmware v03.07 and earlier sold in US. i-SENSYS LBP673Cdw/C1333P/i-SENSYS MF750C Series/C1333i Series firmware v03.07 and earlier sold in Europe.	2024-02-06	9.8	CVE-2023-6231
canon_inc -- satera_lbp670c_series	Buffer overflow in the Address Book username process in authentication of Mobile Device Function of Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code.*: Satera LBP670C Series/Satera MF750C Series firmware v03.07 and earlier sold in Japan. Color imageCLASS LBP674C/Color imageCLASS X LBP1333C/Color imageCLASS MF750C Series/Color imageCLASS X MF1333C Series firmware v03.07 and earlier sold in US. i-SENSYS LBP673Cdw/C1333P/i-SENSYS MF750C Series/C1333i Series firmware v03.07 and earlier sold in Europe.	2024-02-06	9.8	CVE-2023-6232
canon_inc -- satera_lbp670c_series	Buffer overflow in SLP attribute request process of Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code.*: Satera LBP670C Series/Satera MF750C Series firmware v03.07 and earlier sold in Japan. Color imageCLASS LBP674C/Color imageCLASS X LBP1333C/Color imageCLASS MF750C Series/Color imageCLASS X MF1333C Series firmware v03.07 and earlier sold in US. i-SENSYS LBP673Cdw/C1333P/i-SENSYS MF750C Series/C1333i Series firmware v03.07 and earlier sold in Europe.	2024-02-06	9.8	CVE-2023-6233
canon_inc -- satera_lbp670c_series	Buffer overflow in CPCA Color LUT Resource Download process of Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code.*: Satera LBP670C Series/Satera MF750C Series firmware v03.07 and earlier sold in Japan. Color imageCLASS LBP674C/Color imageCLASS X LBP1333C/Color imageCLASS MF750C Series/Color imageCLASS X MF1333C Series firmware v03.07 and earlier sold in US. i-SENSYS LBP673Cdw/C1333P/i-SENSYS MF750C Series/C1333i Series firmware v03.07 and earlier sold in Europe.	2024-02-06	9.8	CVE-2023-6234
canon_inc -- satera_mf750c_series	Buffer overflow in CPCA PCFAX number process of Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code.*:Satera MF750C Series firmware v03.07 and earlier sold in Japan. Color imageCLASS MF750C Series/Color imageCLASS X MF1333C firmware v03.07 and earlier sold in US. i-SENSYS MF754Cdw/C1333iF firmware v03.07 and earlier sold in Europe.	2024-02-06	9.8	CVE-2024-0244
canon_inc -- satera_lbp670c_series	Buffer overflow in CPCA PDL Resource Download process of Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code.*: Satera LBP670C Series/Satera MF750C Series firmware v03.07 and earlier sold in Japan. Color imageCLASS LBP674C/Color imageCLASS X LBP1333C/Color imageCLASS MF750C Series/Color imageCLASS X MF1333C Series firmware v03.07 and earlier sold in US. i-SENSYS LBP673Cdw/C1333P/i-SENSYS MF750C Series/C1333i Series firmware v03.07 and earlier sold in Europe.	2024-02-06	9.8	CVE-2023-6229
canon_inc -- satera_lbp670c_series	Buffer overflow in the Address Book password process in authentication of Mobile Device Function of Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code.*: Satera LBP670C Series/Satera MF750C Series firmware v03.07 and earlier sold in Japan. Color imageCLASS LBP674C/Color imageCLASS X LBP1333C/Color imageCLASS MF750C Series/Color imageCLASS X MF1333C Series firmware v03.07 and earlier sold in US. i-SENSYS	2024-02-06	9.8	CVE-2023-6230

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	LBP673Cdw/C1333P/i-SENSYS MF750C Series/C1333i Series firmware v03.07 and earlier sold in Europe.			
chendotjs -- lotos_webserver	Lotos WebServer v0.1.1 was discovered to contain a Use-After-Free (UAF) vulnerability via the response_append_status_line function at /lotos/src/response.c.	2024-02-05	7.5	CVE-2024-24263
cisco -- cisco_secure_endpoint	A vulnerability in the OLE2 file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to an incorrect check for end-of-string values during scanning, which may result in a heap buffer over-read. An attacker could exploit this vulnerability by submitting a crafted file containing OLE2 content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software and consuming available system resources. For a description of this vulnerability, see the ClamAV blog.	2024-02-07	7.5	CVE-2024-20290
cisco -- cisco_telepresence_video_communication_server_(vcs)_expressway	A vulnerability in the SOAP API of Cisco Expressway Series and Cisco TelePresence Video Communication Server could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected system. An attacker could exploit this vulnerability by persuading a user of the REST API to follow a crafted link. A successful exploit could allow the attacker to cause the affected system to reload.	2024-02-07	8.2	CVE-2024-20255
cisco -- mutiple_products	Multiple vulnerabilities in Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an unauthenticated, remote attacker to conduct cross-site request forgery (CSRF) attacks that perform arbitrary actions on an affected device. Note: "Cisco Expressway Series" refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. For more information about these vulnerabilities, see the Details ["#details"] section of this advisory.	2024-02-07	9.6	CVE-2024-20252
cisco -- mutiple_products	Multiple vulnerabilities in Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an unauthenticated, remote attacker to conduct cross-site request forgery (CSRF) attacks that perform arbitrary actions on an affected device. Note: "Cisco Expressway Series" refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. For more information about these vulnerabilities, see the Details ["#details"] section of this advisory.	2024-02-07	9.6	CVE-2024-20254
composer -- composer	Composer is a dependency Manager for the PHP language. In affected versions several files within the local working directory are included during the invocation of Composer and in the context of the executing user. As such, under certain conditions arbitrary code execution may lead to local privilege escalation, provide lateral user movement or malicious code execution when Composer is invoked within a directory with tampered files. All Composer CLI commands are affected, including composer.phar's self-update. The following scenarios are of high risk: Composer being run with sudo, Pipelines which may execute Composer on untrusted projects, Shared environments with developers who run Composer individually on the same project. This vulnerability has been addressed in versions 2.7.0 and 2.2.23. It is advised that the patched versions are applied at the earliest convenience. Where not possible, the following should be addressed: Remove all sudo composer privileges for all users to mitigate root privilege escalation, and avoid running Composer within an untrusted directory, or if needed, verify that the contents of `vendor/composer/InstalledVersions.php` and `vendor/composer/installed.php` do not include untrusted code. A reset can also be done on these files by the following:```sh rm vendor/composer/installed.php vendor/composer/InstalledVersions.php composer install --no-scripts --no-plugins ```	2024-02-09	8.8	CVE-2024-24821
cpio -- cpio	A path traversal vulnerability was found in the CPIO utility. This issue could allow a remote unauthenticated attacker to trick a user into opening a specially crafted archive. During the extraction process, the archiver could follow symlinks outside of the intended directory, which could be utilized to run arbitrary commands on the target system.	2024-02-05	8.8	CVE-2023-7216
crafty_controller -- crafty_controller	A host header injection vulnerability in the HTTP handler component of Crafty Controller allows a remote, unauthenticated attacker to trigger a Denial of Service (DoS) condition via a modified host header	2024-02-03	7.5	CVE-2024-1064
degamisu -- open-irs	open-irs is an issue response robot that reponds to issues in the installed repository. The `.env` file was accidentally uploaded when working with git actions.	2024-02-02	9.8	CVE-2024-24757

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	This problem is fixed in 1.0.1. Discontinuing all sensitive keys and turning into secrets.			
dell -- bsafe_crypto-c-micro-edition	Dell BSAFE Crypto-C Micro Edition, versions before 4.1.5, and Dell BSAFE Micro Edition Suite, versions before 4.5.2, contain a Missing Required Cryptographic Step Vulnerability.	2024-02-02	9.8	CVE-2020-29504
dell -- bsafe_micro-edition-suite	Dell BSAFE Micro Edition Suite, versions before 4.5.2, contain an Observable Timing Discrepancy Vulnerability.	2024-02-02	9.8	CVE-2021-21575
dell -- bsafe_ssl-j	Dell BSAFE SSL-J version 7.0 and all versions prior to 6.5, and Dell BSAFE Crypto-J versions prior to 6.2.6.1 contain an unmaintained third-party component vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to the compromise of the impacted system. This is a Critical vulnerability and Dell recommends customers to upgrade at the earliest opportunity.	2024-02-02	9.8	CVE-2022-34381
dell -- data_protection_search	Dell Data Protection Search 19.2.0 and above contain an exposed password opportunity in plain text when using LdapSettings.get_ldap_info in DP Search. A remote unauthorized unauthenticated attacker could potentially exploit this vulnerability leading to a loss of Confidentiality, Integrity, Protection, and remote takeover of the system. This is a high-severity vulnerability as it allows an attacker to take complete control of DP Search to affect downstream protected devices.	2024-02-06	8.8	CVE-2024-22433
dell -- dell_display_manager	Dell Display Manager application, version 2.1.1.17, contains a vulnerability that low privilege user can execute malicious code during installation and uninstallation	2024-02-06	7.3	CVE-2023-32451
dell -- dell_power_manager_(dpm)	Dell Power Manager, versions prior to 3.14, contain an Improper Authorization vulnerability in DPM service. A low privileged malicious user could potentially exploit this vulnerability in order to elevate privileges on the system.	2024-02-06	7.8	CVE-2023-25543
diracgrid -- dirac	DIRAC is a distributed resource framework. In affected versions any user could get a token that has been requested by another user/agent. This may expose resources to unintended parties. This issue has been addressed in release version 8.0.37. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-09	9.1	CVE-2024-24825
emerson -- rosemount_gc370xa	In Emerson Rosemount GC370XA, GC700XA, and GC1500XA products, an unauthenticated user with network access could bypass authentication and acquire admin capabilities.	2024-02-09	8.3	CVE-2023-51761
emerson_rosemount-- mutiple products	In Emerson Rosemount GC370XA, GC700XA, and GC1500XA products, an unauthenticated user with network access could execute arbitrary commands in root context from a remote computer.	2024-02-09	9.8	CVE-2023-46687
envoyproxy -- envoy	Envoy is a high-performance edge/middle/service proxy. External authentication can be bypassed by downstream connections. Downstream clients can force invalid gRPC requests to be sent to ext_authz, circumventing ext_authz checks when failure_mode_allow is set to true. This issue has been addressed in released 1.29.1, 1.28.1, 1.27.3, and 1.26.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-09	8.6	CVE-2024-23324
envoyproxy -- envoy	Envoy is a high-performance edge/middle/service proxy. Envoy will crash when certain timeouts happen within the same interval. The crash occurs when the following are true: 1. hedge_on_per_try_timeout is enabled, 2. per_try_idle_timeout is enabled (it can only be done in configuration), 3. per-try-timeout is enabled, either through headers or configuration and its value is equal, or within the backoff interval of the per_try_idle_timeout. This issue has been addressed in released 1.29.1, 1.28.1, 1.27.3, and 1.26.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-09	7.5	CVE-2024-23322
envoyproxy -- envoy	Envoy is a high-performance edge/middle/service proxy. Envoy crashes in Proxy protocol when using an address type that isn't supported by the OS. Envoy is susceptible to crashing on a host with IPv6 disabled and a listener config with proxy protocol enabled when it receives a request where the client presents its IPv6 address. It is valid for a client to present its IPv6 address to a target server even though the whole chain is connected via IPv4. This issue has been addressed in released 1.29.1, 1.28.1, 1.27.3, and 1.26.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-09	7.5	CVE-2024-23325
envoyproxy -- envoy	Envoy is a high-performance edge/middle/service proxy. When PPv2 is enabled both on a listener and subsequent cluster, the Envoy instance will segfault when attempting to craft the upstream PPv2 header. This occurs when the downstream request has a command type of LOCAL and does not have the protocol block. This	2024-02-09	7.5	CVE-2024-23327

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	issue has been addressed in releases 1.29.1, 1.28.1, 1.27.3, and 1.26.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.			
flusity -- flusity	Cross Site Request Forgery vulnerability in flusity-CMS v.2.33 allows a remote attacker to execute arbitrary code via the add_customblock.php.	2024-02-05	8.8	CVE-2024-24468
flusity -- flusity	Cross Site Request Forgery vulnerability in flusity-CMS v.2.33 allows a remote attacker to execute arbitrary code via the delete_post .php.	2024-02-05	8.8	CVE-2024-24469
flusity -- flusity	Cross Site Request Forgery vulnerability in flusity-CMS v.2.33 allows a remote attacker to execute arbitrary code via the update_post.php component.	2024-02-02	8.8	CVE-2024-24470
flusity -- flusity	Cross Site Request Forgery (CSRF) vulnerability in flusity-CMS v.2.33, allows remote attackers to execute arbitrary code via the add_menu.php component.	2024-02-02	8.8	CVE-2024-24524
fortinet -- fortios/fortiproxy	An out-of-bounds write in Fortinet FortiOS versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, 6.0.0 through 6.0.17, FortiProxy versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7 allows attacker to execute unauthorized code or commands via specifically crafted requests	2024-02-09	9.8	CVE-2024-21762
fortinet -- fortisiem	An improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiSIEM version 7.1.0 through 7.1.1 and 7.0.0 through 7.0.2 and 6.7.0 through 6.7.8 and 6.6.0 through 6.6.3 and 6.5.0 through 6.5.2 and 6.4.0 through 6.4.2 allows attacker to execute unauthorized code or commands via via crafted API requests.	2024-02-05	9.8	CVE-2024-23108
fortinet -- fortisiem	An improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiSIEM version 7.1.0 through 7.1.1 and 7.0.0 through 7.0.2 and 6.7.0 through 6.7.8 and 6.6.0 through 6.6.3 and 6.5.0 through 6.5.2 and 6.4.0 through 6.4.2 allows attacker to execute unauthorized code or commands via via crafted API requests.	2024-02-05	9.8	CVE-2024-23109
google -- android	In alac decoder, there is a possible information disclosure due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08441146; Issue ID: ALPS08441146.	2024-02-05	9.8	CVE-2024-20011
google -- android	In alac decoder, there is a possible out of bounds write due to an incorrect error handling. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS08441150; Issue ID: ALPS08441150.	2024-02-05	8.8	CVE-2024-20009
google -- android	In mp3 decoder, there is a possible out of bounds write due to a race condition. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS08441369; Issue ID: ALPS08441369.	2024-02-05	7.5	CVE-2024-20007
google -- android	In telephony, there is a possible escalation of privilege due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08441419; Issue ID: ALPS08441419.	2024-02-05	7.8	CVE-2024-20015
gpac -- gpac	gpac v2.2.1 was discovered to contain a memory leak via the dst_props variable in the gf_filter_pid_merge_properties_internal function.	2024-02-05	7.5	CVE-2024-24265
gpac -- gpac	gpac v2.2.1 was discovered to contain a Use-After-Free (UAF) vulnerability via the dasher_configure_pid function at /src/filters/dasher.c.	2024-02-05	7.5	CVE-2024-24266
gpac -- gpac	gpac v2.2.1 was discovered to contain a memory leak via the gfio_blob variable in the gf_fileio_from_blob function.	2024-02-05	7.5	CVE-2024-24267
graphviz -- graphviz	Graphviz 2.36 before 10.0.0 has an out-of-bounds read via a crafted config6a file. NOTE: exploitability may be uncommon because this file is typically owned by root.	2024-02-02	7.8	CVE-2023-46045
graylog2 -- graylog2_server	Graylog is a free and open log management platform. Starting in version 2.0.0 and prior to versions 5.1.11 and 5.2.4, arbitrary classes can be loaded and instantiated using a HTTP PUT request to the `/api/system/cluster_config/` endpoint. Graylog's cluster config system uses fully qualified class names as config keys. To validate the existence of the requested class before using them, Graylog loads the class using the class loader. If a user with the appropriate permissions performs the request, arbitrary classes with 1-arg String constructors can be instantiated. This will execute arbitrary code that is run during class instantiation. In the specific use case of `java.io.File`, the behavior of the internal web-server stack will lead to information exposure by including the entire file content in the response to the REST request. Versions 5.1.11 and 5.2.4 contain a fix for this issue.	2024-02-07	8.8	CVE-2024-24824

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gttb -- gtb_central_console	An issue was discovered in GTB Central Console 15.17.1-30814.NG. The method setTermsHashAction at /opt/webapp/lib/PureApi/CCApi.class.php is vulnerable to an unauthenticated SQL injection via /ccapi.php that an attacker can abuse in order to change the Administrator password to a known value.	2024-02-02	9.8	CVE-2024-22108
gttb -- gtb_central_console	An issue was discovered in GTB Central Console 15.17.1-30814.NG. The method systemSettingsDnsDataAction at /opt/webapp/src/AppBundle/Controller/React/SystemSettingsController.php is vulnerable to command injection via the /old/react/v1/api/system/dns/data endpoint. An authenticated attacker can abuse it to inject an arbitrary command and compromise the platform.	2024-02-02	7.2	CVE-2024-22107
hashicorp -- boundary	Boundary and Boundary Enterprise ("Boundary") is vulnerable to session hijacking through TLS certificate tampering. An attacker with privileges to enumerate active or pending sessions, obtain a private key pertaining to a session, and obtain a valid trust on first use (TOFU) token may craft a TLS certificate to hijack an active session and gain access to the underlying service or application.	2024-02-05	8	CVE-2024-1052
hashicorp -- nomad	HashiCorp Nomad and Nomad Enterprise 1.5.13 up to 1.6.6, and 1.7.3 template renderer is vulnerable to arbitrary file write on the host as the Nomad client user through symlink attacks. Fixed in Nomad 1.7.4, 1.6.7, 1.5.14.	2024-02-08	7.7	CVE-2024-1329
ibm -- cloud_pak_system	IBM Cloud Pak System 2.3.1.1, 2.3.2.0, and 2.3.3.7 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 260733.	2024-02-02	7.5	CVE-2023-38273
ibm -- engineering_lifecycle_optimization_publishing	IBM Engineering Lifecycle Optimization 7.0.2 and 7.0.3 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 268755.	2024-02-09	7.5	CVE-2023-45191
ibm -- maximo_asset_management	IBM Maximo Asset Management 7.6.1.3 could allow a remote attacker to log into the admin panel due to improper access controls. IBM X-Force ID: 255073.	2024-02-02	9.8	CVE-2023-32333
ibm -- operational_decision_manager	IBM Operational Decision Manager 8.10.3, 8.10.4, 8.10.5.1, 8.11, 8.11.0.1, and 8.12.0.1 is susceptible to remote code execution attack via JNDI injection when passing an unchecked argument to a certain API. IBM X-Force ID: 279145.	2024-02-02	9.8	CVE-2024-22319
ibm -- operational_decision_manager	IBM Operational Decision Manager 8.10.3, 8.10.4, 8.10.5.1, 8.11, 8.11.0.1, and 8.12.0.1 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unsafe deserialization. By sending specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code in the context of SYSTEM. IBM X-Force ID: 279146.	2024-02-02	8.8	CVE-2024-22320
ibm -- powersc	IBM PowerSC 1.3, 2.0, and 2.1 uses Cross-Origin Resource Sharing (CORS) which could allow an attacker to carry out privileged actions and retrieve sensitive information as the domain name is not being limited to only trusted domains. IBM X-Force ID: 275130.	2024-02-02	9.8	CVE-2023-50940
ibm -- powersc	IBM PowerSC 1.3, 2.0, and 2.1 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 275116.	2024-02-02	8.8	CVE-2023-50936
ibm -- powersc	IBM PowerSC 1.3, 2.0, and 2.1 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 275107.	2024-02-02	7.5	CVE-2023-50326
ibm -- powersc	IBM PowerSC 1.3, 2.0, and 2.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 275117.	2024-02-02	7.5	CVE-2023-50937
ibm -- powersc	IBM PowerSC 1.3, 2.0, and 2.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 275129.	2024-02-02	7.5	CVE-2023-50939
ibm -- security_access_manager_container	IBM Security Access Manager Container 10.0.0.0 through 10.0.6.1 does not require that docker images should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 261196.	2024-02-07	7.5	CVE-2023-38369
ibm -- security_verify_access	IBM Security Verify Access 10.0.0.0 through 10.0.6.1 uses insecure protocols in some instances that could allow an attacker on the network to take control of the server. IBM X-Force Id: 254957.	2024-02-07	9.8	CVE-2023-32328
ibm -- security_verify_access	IBM Security Verify Access 10.0.0.0 through 10.0.6.1 uses insecure calls that could allow an attacker on the network to take control of the server. IBM X-Force ID: 254977.	2024-02-07	9.8	CVE-2023-32330
ibm -- security_verify_access	IBM Security Verify Access 10.0.0.0 through 10.0.6.1 could allow a privileged user to install a configuration file that could allow remote access. IBM X-Force ID: 266155.	2024-02-07	7.2	CVE-2023-43017

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_verify_access_appliance/security_verify_access_docker	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 10.0.0.0 through 10.0.6.1) could allow a remote attacker to gain access to the underlying system using man in the middle techniques. IBM X-Force ID: 254765.	2024-02-03	9	CVE-2023-31004
ibm -- security_verify_access_appliance/security_verify_access_docker	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 10.0.0.0 through 10.0.6.1) could allow an attacker to cause a denial of service due to uncontrolled resource consumption. IBM X-Force ID: 254651.	2024-02-03	7.5	CVE-2023-30999
ibm -- security_verify_access_appliance/security_verify_access_docker	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 10.0.0.0 through 10.0.6.1) could allow a local user to escalate their privileges due to an improper security configuration. IBM X-Force ID: 254767.	2024-02-03	7.8	CVE-2023-31005
ibm -- security_verify_access_appliance/security_verify_access_docker	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 10.0.0.0 through 10.0.6.1) is vulnerable to a denial of service attacks on the DSC server. IBM X-Force ID: 254776.	2024-02-03	7.5	CVE-2023-31006
ibm -- security_verify_access_appliance/security_verify_access_docker	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 10.0.0.0 through 10.0.6.1) is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 254783.	2024-02-03	7.1	CVE-2023-32327
ibm -- security_verify_access_appliance/security_verify_access_docker	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 10.0.0.0 through 10.0.6.1) could allow a remote user to log into the server due to a user account with an empty password. IBM X-Force ID: 266154.	2024-02-03	7.3	CVE-2023-43016
ibm -- soar_qradar_plugin_app	IBM SOAR QRadar Plugin App 1.0 through 5.0.3 could allow an authenticated user to perform unauthorized actions due to improper access controls. IBM X-Force ID: 260577.	2024-02-02	8.8	CVE-2023-38263
ibm -- spectrum_protect_plus	IBM Storage Protect Plus Server 10.1.0 through 10.1.15.2 Admin Console could allow a remote attacker to obtain sensitive information due to improper validation of unsecured endpoints which could be used in further attacks against the system. IBM X-Force ID: 270599.	2024-02-02	7.5	CVE-2023-47148
ibm -- storage_defender_--_resiliency_service	IBM Storage Defender - Resiliency Service 2.0 could allow a privileged user to perform unauthorized actions after obtaining encrypted data from clear text key storage. IBM X-Force ID: 275783.	2024-02-10	8	CVE-2023-50957
ibm -- tivoli_application_dependency_discovery_manager	IBM Tivoli Application Dependency Discovery Manager 7.3.0.0 through 7.3.0.10 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: 270270.	2024-02-02	9.8	CVE-2023-47143
ibm -- tivoli_application_dependency_discovery_manager	IBM Tivoli Application Dependency Discovery Manager 7.3.0.0 through 7.3.0.10 could allow an attacker on the organization's local network to escalate their privileges due to unauthorized API access. IBM X-Force ID: 270267.	2024-02-02	8.8	CVE-2023-47142
icinga -- icingaweb2_module_director	Icinga Director is a tool designed to make Icinga 2 configuration handling easy. Not any of Icinga Director's configuration forms used to manipulate the monitoring environment are protected against cross site request forgery (CSRF). It enables attackers to perform changes in the monitoring environment managed by Icinga Director without the awareness of the victim. Users of the map module in version 1.x, should immediately upgrade to v2.0. The mentioned XSS vulnerabilities in Icinga Web are already fixed as well and upgrades to the most recent release of the 2.9, 2.10 or 2.11 branch must be performed if not done yet. Any later major release is also suitable. Icinga Director will receive minor updates to the 1.8, 1.9, 1.10 and 1.11 branches to remedy this issue. Upgrade immediately to a patched release. If that is not feasible, disable the director module for the time being.	2024-02-09	8.3	CVE-2024-24820
ireader -- media-server	media-server v1.0.0 was discovered to contain a Use-After-Free (UAF) vulnerability via the sip_subscribe_remove function at /uac/sip-uac-subscribe.c.	2024-02-05	7.5	CVE-2024-24260

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ireader -- media-server	media-server v1.0.0 was discovered to contain a Use-After-Free (UAF) vulnerability via the sip_uac_stop_timer function at /uac/sip-uac-transaction.c.	2024-02-05	7.5	CVE-2024-24262
jetbrains -- teamcity	In JetBrains TeamCity before 2023.11.3 authentication bypass leading to RCE was possible	2024-02-06	9.8	CVE-2024-23917
jfinalcms_project -- jfinalcms	JFinalCMS 5.0.0 is vulnerable to SQL injection via /admin/content/data.	2024-02-02	9.8	CVE-2024-24029
jishenghua -- jsherp	jshERP v3.3 is vulnerable to SQL Injection. via the com.jsh.erp.controller.DepotHeadController: com.jsh.erp.utils.BaseResponseInfo findallocationDetail() function of jshERP which allows an attacker to construct malicious payload to bypass jshERP's protection mechanism.	2024-02-07	9.8	CVE-2024-24001
jishenghua -- jsherp	jshERP v3.3 is vulnerable to SQL Injection. The com.jsh.erp.controller.MaterialController: com.jsh.erp.utils.BaseResponseInfo getListWithStock() function of jshERP does not filter `column` and `order` parameters well enough, and an attacker can construct malicious payload to bypass jshERP's protection mechanism in `safeSqlParse` method for sql injection.	2024-02-07	9.8	CVE-2024-24002
jishenghua -- jsherp	jshERP v3.3 is vulnerable to SQL Injection. The com.jsh.erp.controller.DepotHeadController: com.jsh.erp.utils.BaseResponseInfo findInOutMaterialCount() function of jshERP does not filter `column` and `order` parameters well enough, and an attacker can construct malicious payload to bypass jshERP's protection mechanism in `safeSqlParse` method for sql injection.	2024-02-08	9.8	CVE-2024-24003
jishenghua -- jsherp	jshERP v3.3 is vulnerable to SQL Injection. The com.jsh.erp.controller.DepotHeadController: com.jsh.erp.utils.BaseResponseInfo findInOutDetail() function of jshERP does not filter `column` and `order` parameters well enough, and an attacker can construct malicious payload to bypass jshERP's protection mechanism in `safeSqlParse` method for sql injection.	2024-02-07	9.8	CVE-2024-24004
jsish -- jsish	Jsish v3.5.0 (commit 42c694c) was discovered to contain a stack-overflow via the component IterGetKeysCallback at /jsish/src/jsiValue.c.	2024-02-07	9.8	CVE-2024-24186
jsish -- jsish	Jsish v3.5.0 was discovered to contain a heap-buffer-overflow in ./src/jsiUtils.c.	2024-02-07	9.8	CVE-2024-24188
jsish -- jsish	Jsish v3.5.0 (commit 42c694c) was discovered to contain a use-after-free via the SplitChar at ./src/jsiUtils.c.	2024-02-07	9.8	CVE-2024-24189
kddi -- home_spot_cube_2_firmware	Heap-based buffer overflow vulnerability exists in HOME SPOT CUBE2 V102 and earlier. By processing invalid values, arbitrary code may be executed. Note that the affected products are no longer supported.	2024-02-02	9.8	CVE-2024-23978
kddi -- home_spot_cube_2_firmware	Stack-based buffer overflow vulnerability exists in HOME SPOT CUBE2 V102 and earlier. Processing a specially crafted command may result in a denial of service (DoS) condition. Note that the affected products are no longer supported.	2024-02-02	7.5	CVE-2024-21780
kihron -- serverrpexposer	Directory Traversal vulnerability in Kihron ServerRPExposer v.1.0.2 and before allows a remote attacker to execute arbitrary code via the loadServerPack in ServerResourcePackProviderMixin.java.	2024-02-02	9.8	CVE-2024-22779
ledgersmb -- ledgersmb	LedgerSMB is a free web-based double-entry accounting system. When a LedgerSMB database administrator has an active session in /setup.pl, an attacker can trick the admin into clicking on a link which automatically submits a request to setup.pl without the admin's consent. This request can be used to create a new user account with full application (/login.pl) privileges, leading to privilege escalation. The vulnerability is patched in versions 1.10.30 and 1.11.9.	2024-02-02	7.5	CVE-2024-23831
libexpat_project -- libexpat	libexpat through 2.5.0 allows a denial of service (resource consumption) because many full reparsings are required in the case of a large token for which multiple buffer fills are needed.	2024-02-04	7.5	CVE-2023-52425
libgit2 -- libgit2	libgit2 is a portable C implementation of the Git core methods provided as a linkable library with a solid API, allowing to build Git functionality into your application. Using well-crafted inputs to `git_index_add` can cause heap corruption that could be leveraged for arbitrary code execution. There is an issue in the `has_dir_name` function in `src/libgit2/index.c`, which frees an entry that should not be freed. The freed entry is later used and overwritten with potentially bad actor-controlled data leading to controlled heap corruption. Depending on the application that uses libgit2, this could lead to arbitrary code execution. This issue has been patched in version 1.6.5 and 1.7.2.	2024-02-06	8.6	CVE-2024-24577
libgit2 -- libgit2	libgit2 is a portable C implementation of the Git core methods provided as a linkable library with a solid API, allowing to build Git functionality into your application. Using well-crafted inputs to `git_revparse_single` can cause the function to enter an infinite loop, potentially causing a Denial of Service attack in the calling application. The revparse function in `src/libgit2/revparse.c` uses a loop to parse the user-provided spec string. There is an edge-case during parsing that allows a bad actor to force the loop conditions to access arbitrary memory.	2024-02-06	7.5	CVE-2024-24575

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Potentially, this could also leak memory if the extracted rev spec is reflected back to the attacker. As such, libgit2 versions before 1.4.0 are not affected. Users should upgrade to version 1.6.5 or 1.7.2.			
libuv -- libuv	libuv is a multi-platform support library with a focus on asynchronous I/O. The `uv_getaddrinfo` function in `src/unix/getaddrinfo.c` (and its windows counterpart `src/win/getaddrinfo.c`), truncates hostnames to 256 characters before calling `getaddrinfo`. This behavior can be exploited to create addresses like `0x00007f000001`, which are considered valid by `getaddrinfo` and could allow an attacker to craft payloads that resolve to unintended IP addresses, bypassing developer checks. The vulnerability arises due to how the `hostname_ascii` variable (with a length of 256 bytes) is handled in `uv_getaddrinfo` and subsequently in `uv__idna_toascii`. When the hostname exceeds 256 characters, it gets truncated without a terminating null byte. As a result attackers may be able to access internal APIs or for websites (similar to MySpace) that allows users to have `username.example.com` pages. Internal services that crawl or cache these user pages can be exposed to SSRF attacks if a malicious user chooses a long vulnerable username. This issue has been addressed in release version 1.48.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-07	7.3	CVE-2024-24806
liferay -- portal/dxp	Stored cross-site scripting (XSS) vulnerability in the Portal Search module's Search Result app in Liferay Portal 7.2.0 through 7.4.3.11, and older unsupported versions, and Liferay DXP 7.4 before update 8, 7.3 before update 4, 7.2 before fix pack 17, and older unsupported versions allows remote authenticated users to inject arbitrary web script or HTML into the Search Result app's search result if highlighting is disabled by adding any searchable content (e.g., blog, message board message, web content article) to the application.	2024-02-07	9.6	CVE-2024-25145
liveconfig -- liveconfig	Directory Traversal Vulnerability in LiveConfig before v.2.5.2 allows a remote attacker to obtain sensitive information via a crafted request to the /static/ endpoint.	2024-02-02	7.5	CVE-2024-22851
magic_hills_pty_ltd -- wonder_slider_lite	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Magic Hills Pty Ltd Wonder Slider Lite allows Reflected XSS. This issue affects Wonder Slider Lite: from n/a through 13.9.	2024-02-08	7.1	CVE-2024-24877
mailcow -- mailcow-dockerized	mailcow is a dockerized email package, with multiple containers linked in one bridged network. A security vulnerability has been identified in mailcow affecting versions < 2024-01c. This vulnerability potentially allows attackers on the same subnet to connect to exposed ports of a Docker container, even when the port is bound to 127.0.0.1. The vulnerability has been addressed by implementing additional iptables/nftables rules. These rules drop packets for Docker containers on ports 3306, 6379, 8983, and 12345, where the input interface is not `br-mailcow` and the output interface is `br-mailcow`.	2024-02-02	7.3	CVE-2024-24760
mate_desktop -- engrampa	Engrampa is an archive manager for the MATE environment. Engrampa is found to be vulnerable to a Path Traversal vulnerability that can be leveraged to achieve full Remote Command Execution (RCE) on the target. While handling CPIO archives, the Engrampa Archive manager follows symlink, cpio by default will follow stored symlinks while extracting and the Archiver will not check the symlink location, which leads to arbitrary file writes to unintended locations. When the victim extracts the archive, the attacker can craft a malicious cpio or ISO archive to achieve RCE on the target system. This vulnerability was fixed in commit 63d5dfa.	2024-02-05	8.2	CVE-2023-52138
mediatek -- nr15	In Modem NL1, there is a possible system crash due to an improper input validation. This could lead to remote denial of service, if NW sent invalid NR RRC Connection Setup message, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01191612; Issue ID: MOLY01191612 (MSV-981).	2024-02-05	7.5	CVE-2024-20003
mediatek -- nr15	In Modem NL1, there is a possible system crash due to an improper input validation. This could lead to remote denial of service, if NW sent invalid NR RRC Connection Setup message, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01191612; Issue ID: MOLY01195812 (MSV-985).	2024-02-05	7.5	CVE-2024-20004
meshcentral -- meshcentral	Ylianst MeshCentral 1.1.16 suffers from Use of a Broken or Risky Cryptographic Algorithm.	2024-02-02	7.5	CVE-2023-51838
mia_technology_inc. -- mia-med	Exposure of Sensitive Information Due to Incompatible Policies vulnerability in Mia Technology Inc. MİA-MED allows Collect Data as Provided by Users. This issue affects MİA-MED: before 1.0.7.	2024-02-08	7.5	CVE-2023-6517

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mia_technology_inc. -- mia-med	Plaintext Storage of a Password vulnerability in Mia Technology Inc. MİA-MED allows Read Sensitive Strings Within an Executable. This issue affects MİA-MED: before 1.0.7.	2024-02-08	7.5	CVE-2023-6518
mia_technology_inc. -- mia-med	Exposure of Data Element to Wrong Session vulnerability in Mia Technology Inc. MİA-MED allows Read Sensitive Strings Within an Executable. This issue affects MİA-MED: before 1.0.7.	2024-02-08	7.5	CVE-2023-6519
mia_technology_inc -- mia-med	Authorization Bypass Through User-Controlled Key vulnerability in Mia Technology Inc. MİA-MED allows Authentication Abuse. This issue affects MİA-MED: before 1.0.7.	2024-02-08	8.8	CVE-2023-6515
microsoft -- edge_chromium	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2024-02-02	8.3	CVE-2024-21399
miro -- miro	Miro Desktop 0.8.18 on macOS allows Electron code injection.	2024-02-02	9.8	CVE-2024-23746
mrcms -- mrcms	MRCMS 3.0 contains an Arbitrary File Read vulnerability in /admin/file/edit.do as the incoming path parameter is not filtered.	2024-02-02	7.5	CVE-2024-24161
nationalkeep -- cybermath	Unrestricted Upload of File with Dangerous Type vulnerability in National Keep Cyber Security Services CyberMath allows Upload a Web Shell to a Web Server. This issue affects CyberMath: from v.1.4 before v.1.5.	2024-02-02	9.8	CVE-2023-6675
nationalkeep -- cybermath	Cross-Site Request Forgery (CSRF) vulnerability in National Keep Cyber Security Services CyberMath allows Cross Site Request Forgery. This issue affects CyberMath: from v1.4 before v1.5.	2024-02-02	8.8	CVE-2023-6676
oduyo -- financial_technology_online_collection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Oduyo Financial Technology Online Collection allows SQL Injection. This issue affects Online Collection: before v.1.0.2.	2024-02-09	9.8	CVE-2023-6677
open_formulieren -- open_forms	Open Forms allows users create and publish smart forms. Versions prior to 2.2.9, 2.3.7, 2.4.5, and 2.5.2 contain a non-exploitable multi-factor authentication weakness. Superusers who have their credentials (username + password) compromised could potentially have the second-factor authentication bypassed if an attacker somehow managed to authenticate to Open Forms. The maintainers of Open Forms do not believe it is or has been possible to perform this login. However, if this were possible, the victim's account may be abused to view (potentially sensitive) submission data or have been used to impersonate other staff accounts to view and/or modify data. Three mitigating factors to help prevent exploitation include: the usual login page (at `/admin/login/`) does not fully log in the user until the second factor was succesfully provided; the additional non-MFA protected login page at `/api/v2/api-authlogin/` was misconfigured and could not be used to log in; and there are no additional ways to log in. This also requires credentials of a superuser to be compromised to be exploitable. Versions 2.2.9, 2.3.7, 2.4.5, and 2.5.2 contain the following patches to address these weaknesses: Move and only enable the API auth endpoints (`/api/v2/api-auth/login/`) with `settings.DEBUG = True`. `settings.DEBUG = True` is insecure and should never be applied in production settings. Additionally, apply a custom permission check to the hijack flow to only allow second-factor-verified superusers to perform user hijacking.	2024-02-07	7.7	CVE-2024-24771
openharmony -- openharmony	in OpenHarmony v3.2.4 and prior versions allow an adjacent attacker arbitrary code execution through out-of-bounds write.	2024-02-02	8.8	CVE-2023-45734
openharmony -- openharmony	in OpenHarmony v4.0.0 and prior versions allow an adjacent attacker arbitrary code execution in any apps through use after free.	2024-02-02	8.8	CVE-2024-21860
openharmony -- openharmony	in OpenHarmony v4.0.0 and prior versions allow a local attacker cause heap overflow through integer overflow.	2024-02-02	7.8	CVE-2024-21845
openharmony -- openharmony	in OpenHarmony v4.0.0 and prior versions allow a local attacker cause heap overflow through integer overflow.	2024-02-02	7.8	CVE-2024-21851
openobserve -- openobserve	OpenObserve is a observability platform built specifically for logs, metrics, traces, analytics, designed to work at petabyte scale. A vulnerability has been identified in the "/api/{org_id}/users" endpoint. This vulnerability allows any authenticated regular user ('member') to add new users with elevated privileges, including the 'root' role, to an organization. This issue circumvents the intended security controls for role assignments. The vulnerability resides in the user creation process, where the payload does not validate the user roles. A regular user can manipulate the payload to assign root-level privileges. This vulnerability leads to Unauthorized Privilege Escalation and significantly compromises the application's role-based access control system. It allows unauthorized control over application resources	2024-02-08	9.9	CVE-2024-24830

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and poses a risk to data security. All users, particularly those in administrative roles, are impacted. This issue has been addressed in release version 0.8.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.			
openobserve -- openobserve	OpenObserve is a observability platform built specifically for logs, metrics, traces, analytics, designed to work at petabyte scale. A critical vulnerability has been identified in the "/api/{org_id}/users/{email_id}" endpoint. This vulnerability allows any authenticated user within an organization to remove any other user from that same organization, irrespective of their respective roles. This includes the ability to remove users with "Admin" and "Root" roles. By enabling any organizational member to unilaterally alter the user base, it opens the door to unauthorized access and can cause considerable disruptions in operations. The core of the vulnerability lies in the `remove_user_from_org` function in the user management system. This function is designed to allow organizational users to remove members from their organization. The function does not check if the user initiating the request has the appropriate administrative privileges to remove a user. Any user who is part of the organization, irrespective of their role, can remove any other user, including those with higher privileges. This vulnerability is categorized as an Authorization issue leading to Unauthorized User Removal. The impact is severe, as it compromises the integrity of user management within organizations. By exploiting this vulnerability, any user within an organization, without the need for administrative privileges, can remove critical users, including "Admins" and "Root" users. This could result in unauthorized system access, administrative lockout, or operational disruptions. Given that user accounts are typically created by "Admins" or "Root" users, this vulnerability can be exploited by any user who has been granted access to an organization, thereby posing a critical risk to the security and operational stability of the application. This issue has been addressed in release version 0.8.0. Users are advised to upgrade.	2024-02-08	9.1	CVE-2024-25106
panterasoft -- hdd_health	Search path or unquoted item vulnerability in HDD Health affecting versions 4.2.0.112 and earlier. This vulnerability could allow a local attacker to store a malicious executable file within the unquoted search path, resulting in privilege escalation.	2024-02-02	7.8	CVE-2024-1201
ping_identity -- pingfederate	Authentication bypass when an OAuth2 Client is using client_secret_jwt as its authentication method on affected 11.3 versions via specially crafted requests.	2024-02-06	8.8	CVE-2023-40545
postgresql -- postgresql	Late privilege drop in REFRESH MATERIALIZED VIEW CONCURRENTLY in PostgreSQL allows an object creator to execute arbitrary SQL functions as the command issuer. The command intends to run SQL functions as the owner of the materialized view, enabling safe refresh of untrusted materialized views. The victim is a superuser or member of one of the attacker's roles. The attack requires luring the victim into running REFRESH MATERIALIZED VIEW CONCURRENTLY on the attacker's materialized view. As part of exploiting this vulnerability, the attacker creates functions that use CREATE RULE to convert the internally-built temporary table to a view. Versions before PostgreSQL 15.6, 14.11, 13.14, and 12.18 are affected. The only known exploit does not work in PostgreSQL 16 and later. For defense in depth, PostgreSQL 16.2 adds the protections that older branches are using to fix their vulnerability.	2024-02-08	8	CVE-2024-0985
pt_woo_plugins_(by_webdados) -- portugal_ctt_tracking_for_woocommerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PT Woo Plugins (by Webdados) Portugal CTT Tracking for WooCommerce allows Reflected XSS. This issue affects Portugal CTT Tracking for WooCommerce: from n/a through 2.1.	2024-02-08	7.1	CVE-2024-24878
qibosoft -- qibocms_x1	A vulnerability classified as critical was found in QiboSoft QiboCMS X1 up to 1.0.6. Affected by this vulnerability is the function rmb_pay of the file /application/index/controller/Pay.php. The manipulation of the argument callback_class leads to deserialization. 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-252847. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-05	7.3	CVE-2024-1225
qnap -- photo_station	An OS command injection vulnerability has been reported to affect Photo Station. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following version: Photo Station 6.4.2 (2023/12/15) and later	2024-02-02	8.8	CVE-2023-47562
qnap -- qsync_central	An incorrect permission assignment for critical resource vulnerability has been reported to affect Qsync Central. If exploited, the vulnerability could allow	2024-02-02	8.1	CVE-2023-47564

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authenticated users to read or modify the resource via a network. We have already fixed the vulnerability in the following versions: Qsync Central 4.4.0.15 (2024/01/04) and later Qsync Central 4.3.0.11 (2024/01/11) and later			
qnap -- qts	An improper authentication vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to compromise the security of the system 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 QuTScloud c5.1.5.2651 and later	2024-02-02	9.8	CVE-2023-39303
qnap -- qts	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.4.2596 build 20231128 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later	2024-02-02	9.8	CVE-2023-45025
qnap -- qts	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.4.2596 build 20231128 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later	2024-02-02	8.8	CVE-2023-39297
qnap -- qts	A SQL injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.5.2645 build 20240116 and later QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.5.2647 build 20240118 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later	2024-02-02	8.8	CVE-2023-47568
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 QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	CVE-2023-39302
qnap -- qts	A heap-based buffer overflow 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 5.1.2.2533 build 20230926 and later QuTS hero h5.1.2.2534 build 20230927 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	CVE-2023-41273
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 5.1.2.2533 build 20230926 and later QuTS hero h5.1.2.2534 build 20230927 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	CVE-2023-41275
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 5.1.2.2533 build 20230926 and later QuTS hero h5.1.2.2534 build 20230927 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	CVE-2023-41276
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 5.1.2.2533 build 20230926 and later QuTS hero h5.1.2.2534 build 20230927 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	CVE-2023-41277
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 5.1.2.2533 build 20230926 and later QuTS hero h5.1.2.2534 build 20230927 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	CVE-2023-41278
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 5.1.2.2533 build	2024-02-02	7.2	CVE-2023-41279

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	20230926 and later QuTS hero h5.1.2.2534 build 20230927 and later QuTScloud c5.1.5.2651 and later			
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 5.1.2.2533 build 20230926 and later QuTS hero h5.1.2.2534 build 20230927 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	CVE-2023-41280
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 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	CVE-2023-41281
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 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	CVE-2023-41282
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 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	CVE-2023-41283
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 QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	CVE-2023-41292
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 QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	CVE-2023-45035
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 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	CVE-2023-45036
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 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	CVE-2023-45037
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 5.1.5.2645 build 20240116 and later QuTS hero h5.1.5.2647 build 20240118 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	CVE-2023-47566
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 5.1.5.2645 build 20240116 and later QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.5.2647 build 20240118 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later	2024-02-02	7.2	CVE-2023-47567
qolsys_inc -- iq_panel_4	Under certain circumstances IQ Panel4 and IQ4 Hub panel software prior to version 4.4.2 could allow unauthorized access to settings.	2024-02-08	7.3	CVE-2024-0242
qualcomm -- 315_5g_iot_modem_firmware	Transient DOS in Multi-Mode Call Processor due to UE failure because of heap leakage.	2024-02-06	7.5	CVE-2023-33049

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qualcomm -- 315_5g_iot_modem_firmware	Transient DOS in Multi-Mode Call Processor while processing UE policy container.	2024-02-06	7.5	CVE-2023-33057
qualcomm -- 315_5g_iot_modem_firmware	Memory corruption in Core while processing control functions.	2024-02-06	7.8	CVE-2023-33072
qualcomm -- 315_5g_iot_modem_firmware	Memory corruption while processing the event ring, the context read pointer is untrusted to HLOS and when it is passed with arbitrary values, may point to address in the middle of ring element.	2024-02-06	7.8	CVE-2023-43513
qualcomm -- 315_5g_iot_modem_firmware	Transient DOS in WLAN Firmware when the length of received beacon is less than length of ieee802.11 beacon frame.	2024-02-06	7.5	CVE-2023-43533
qualcomm -- 315_5g_iot_modem_firmware	Transient DOS while parse fils IE with length equal to 1.	2024-02-06	7.5	CVE-2023-43536
qualcomm -- 9206_lte_modem_firmware	Memory corruption in Audio while calling START command on host voice PCM multiple times for the same RX or TX tap points.	2024-02-06	7.8	CVE-2023-33067
qualcomm -- 9206_lte_modem_firmware	Memory corruption in Audio while processing IIR config data from AFE calibration block.	2024-02-06	7.8	CVE-2023-33068
qualcomm -- 9206_lte_modem_firmware	Memory corruption in Audio while processing the calibration data returned from ACDB loader.	2024-02-06	7.8	CVE-2023-33069
qualcomm -- aqt1000_firmware	Memory corruption in video while parsing invalid mp2 clip.	2024-02-06	9.8	CVE-2023-43518
qualcomm -- aqt1000_firmware	Memory corruption in video while parsing the Videoinfo, when the size of atom is greater than the videoinfo size.	2024-02-06	9.8	CVE-2023-43519
qualcomm -- aqt1000_firmware	Information disclosure in Audio while accessing AVCS services from ADSP payload.	2024-02-06	7.1	CVE-2023-33065
qualcomm -- aqt1000_firmware	Memory corruption in Core when updating rollback version for TA and OTA feature is enabled.	2024-02-06	7.8	CVE-2023-33076
qualcomm -- aqt1000_firmware	Memory corruption in HLOS while converting from authorization token to HIDL vector.	2024-02-06	7.8	CVE-2023-33077
qualcomm -- aqt1000_firmware	Transient DOS while key unwrapping process, when the given encrypted key is empty or NULL.	2024-02-06	7.5	CVE-2023-43522
qualcomm -- ar8035_firmware	Information disclosure in Modem while processing SIB5.	2024-02-06	9.1	CVE-2023-33058
qualcomm -- ar8035_firmware	Memory corruption when AP includes TID to link mapping IE in the beacons and STA is parsing the beacon TID to link mapping IE.	2024-02-06	9.8	CVE-2023-43520
qualcomm -- ar8035_firmware	Memory corruption while validating the TID to Link Mapping action request frame, when a station connects to an access point.	2024-02-06	9.8	CVE-2023-43534
qualcomm -- ar8035_firmware	Memory corruption in Trusted Execution Environment while deinitializing an object used for license validation.	2024-02-06	7	CVE-2023-33046
qualcomm -- ar8035_firmware	Transient DOS while processing 11AZ RTT management action frame received through OTA.	2024-02-06	7.5	CVE-2023-43523
qualcomm -- fastconnect_6700_firmware	Memory corruption while reading ACPI config through the user mode app.	2024-02-06	7.8	CVE-2023-43532
qualcomm -- fastconnect_6700_firmware	Memory corruption when negative display IDs are sent as input while processing DISPLAYESCAPE event trigger.	2024-02-06	7.8	CVE-2023-43535
qualcomm -- fastconnect_6900_firmware	Memory corruption when malformed message payload is received from firmware.	2024-02-06	7.8	CVE-2023-43516
qualcomm -- qam8255p_firmware	Memory corruption in Automotive Multimedia due to improper access control in HAB.	2024-02-06	7.8	CVE-2023-43517
rapidscada -- rapid_scada	In Rapid Software LLC's Rapid SCADA versions prior to Version 5.8.4, the product uses hard-coded credentials, which may allow an attacker to connect to a specific port.	2024-02-02	9.8	CVE-2024-21764
rapidscada -- rapid_scada	In Rapid Software LLC's Rapid SCADA versions prior to Version 5.8.4, an authorized user can write directly to the Scada directory. This may allow privilege escalation.	2024-02-02	7.8	CVE-2024-22016

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
remyandrade -- testimonial_page_manager	A vulnerability, which was classified as critical, has been found in SourceCodester Testimonial Page Manager 1.0. This issue affects some unknown processing of the file delete-testimonial.php of the component HTTP GET Request Handler. The manipulation of the argument testimony leads to sql injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-252695.	2024-02-02	9.8	CVE-2024-1197
samsung -- magician_pc_software	Improper privilege control for the named pipe in Samsung Magician PC Software 8.0.0 (for Windows) allows a local attacker to read privileged data.	2024-02-07	7.3	CVE-2024-23769
samsung_mobile -- samsung_mobile_devices	Out-of-bounds Write in padmd_vld_htbl of libpadm.so prior to SMR Feb-2024 Release 1 allows local attacker to execute arbitrary code.	2024-02-06	8.4	CVE-2024-20812
samsung_mobile -- samsung_mobile_devices	Out-of-bounds Write in padmd_vld_qtbl of libpadm.so prior to SMR Feb-2024 Release 1 allows local attacker to execute arbitrary code.	2024-02-06	8.4	CVE-2024-20813
samsung_mobile -- samsung_mobile_devices	Improper authentication vulnerability in onCharacteristicReadRequest in Auto Hotspot prior to SMR Feb-2024 Release 1 allows adjacent attackers connect to victim's mobile hotspot without user awareness.	2024-02-06	8	CVE-2024-20815
samsung_mobile -- samsung_mobile_devices	Improper authentication vulnerability in onCharacteristicWriteRequest in Auto Hotspot prior to SMR Feb-2024 Release 1 allows adjacent attackers connect to victim's mobile hotspot without user awareness.	2024-02-06	8	CVE-2024-20816
silabs -- gecko_software_development_kit	A potential buffer overflow exists in the Bluetooth LE HCI CPC sample application in the Gecko SDK which may result in a denial of service or remote code execution	2024-02-02	7.5	CVE-2023-6387
silabs -- gecko_software_development_kit	Prior to v7.4.0, Ember ZNet is vulnerable to a denial of service attack through manipulation of the NWK sequence number	2024-02-05	7.5	CVE-2023-6874
snow_software -- inventory_agent	Improper Verification of Cryptographic Signature vulnerability in Snow Software Inventory Agent on MacOS, Snow Software Inventory Agent on Windows, Snow Software Inventory Agent on Linux allows File Manipulation through Snow Update Packages. This issue affects Inventory Agent: through 6.12.0; Inventory Agent: through 6.14.5; Inventory Agent: through 6.7.2.	2024-02-08	7.8	CVE-2024-1149
snow_software -- inventory_agent	Improper Verification of Cryptographic Signature vulnerability in Snow Software Inventory Agent on Unix allows File Manipulation through Snow Update Packages. This issue affects Inventory Agent: through 7.3.1.	2024-02-08	7.8	CVE-2024-1150
software_engineering_consultancy_machine_equipment_limited_company -- hearing_tracking_system	Authorization Bypass Through User-Controlled Key vulnerability in Software Engineering Consultancy Machine Equipment Limited Company Hearing Tracking System allows Authentication Abuse. This issue affects Hearing Tracking System: before for IOS 7.0, for Android Latest release 1.0.	2024-02-09	8.8	CVE-2023-6724
softwarefx -- chart_fx	An issue in Software FX Chart FX 7 version 7.0.4962.20829 allows attackers to enumerate and read files from the local filesystem by sending crafted web requests.	2024-02-02	7.5	CVE-2023-39611
solarwinds -- solarwinds_platform	SQL Injection Remote Code Execution Vulnerability was found using an update statement in the SolarWinds Platform. This vulnerability requires user authentication to be exploited	2024-02-06	8	CVE-2023-50395
solarwinds -- solarwinds_platform	SQL Injection Remote Code Execution Vulnerability was found using a create statement in the SolarWinds Platform. This vulnerability requires user authentication to be exploited.	2024-02-06	8	CVE-2023-35188
tiangolo -- fastapi	FastAPI is a web framework for building APIs with Python 3.8+ based on standard Python type hints. When using form data, `python-multipart` uses a Regular Expression to parse the HTTP `Content-Type` header, including options. An attacker could send a custom-made `Content-Type` option that is very difficult for the RegEx to process, consuming CPU resources and stalling indefinitely (minutes or more) while holding the main event loop. This means that process can't handle any more requests. It's a ReDoS(Regular expression Denial of Service), it only applies to those reading form data, using `python-multipart`. This vulnerability has been patched in version 0.109.1.	2024-02-05	7.5	CVE-2024-24762
tp-link -- er7206_firmware	A post-authentication command injection vulnerability exists in the PPTP client functionality of Tp-Link ER7206 Omada Gigabit VPN Router 1.3.0 build 20230322 Rel.70591. A specially crafted HTTP request can lead to arbitrary command injection. An attacker can make an authenticated HTTP request to trigger this vulnerability and gain access to an unrestricted shell.	2024-02-06	7.2	CVE-2023-36498

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tp-link -- er7206_firmware	A post authentication command injection vulnerability exists when setting up the PPTP global configuration of Tp-Link ER7206 Omada Gigabit VPN Router 1.3.0 build 20230322 Rel.70591. A specially crafted HTTP request can lead to arbitrary command injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2024-02-06	7.2	CVE-2023-42664
tp-link -- er7206_firmware	A command execution vulnerability exists in the guest resource functionality of Tp-Link ER7206 Omada Gigabit VPN Router 1.3.0 build 20230322 Rel.70591. A specially crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2024-02-06	7.2	CVE-2023-43482
tp-link -- er7206_firmware	A post authentication command injection vulnerability exists when configuring the wireguard VPN functionality of Tp-Link ER7206 Omada Gigabit VPN Router 1.3.0 build 20230322 Rel.70591. A specially crafted HTTP request can lead to arbitrary command injection . An attacker can make an authenticated HTTP request to trigger this vulnerability.	2024-02-06	7.2	CVE-2023-46683
tp-link -- er7206_firmware	A post authentication command injection vulnerability exists in the GRE policy functionality of Tp-Link ER7206 Omada Gigabit VPN Router 1.3.0 build 20230322 Rel.70591. A specially crafted HTTP request can lead to arbitrary command injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2024-02-06	7.2	CVE-2023-47167
tp-link -- er7206_firmware	A post authentication command injection vulnerability exists in the ipsec policy functionality of Tp-Link ER7206 Omada Gigabit VPN Router 1.3.0 build 20230322 Rel.70591. A specially crafted HTTP request can lead to arbitrary command injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2024-02-06	7.2	CVE-2023-47209
tp-link -- er7206_firmware	A post authentication command injection vulnerability exists when configuring the web group member of Tp-Link ER7206 Omada Gigabit VPN Router 1.3.0 build 20230322 Rel.70591. A specially crafted HTTP request can lead to arbitrary command injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2024-02-06	7.2	CVE-2023-47617
tp-link -- er7206_firmware	A post authentication command execution vulnerability exists in the web filtering functionality of Tp-Link ER7206 Omada Gigabit VPN Router 1.3.0 build 20230322 Rel.70591. A specially crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2024-02-06	7.2	CVE-2023-47618
vinchin -- vinchin_backup_and_recovery	Vinchin Backup & Recovery v7.2 was discovered to use default MYSQL credentials.	2024-02-02	9.8	CVE-2024-22901
vinchin -- vinchin_backup_and_recovery	Vinchin Backup & Recovery v7.2 was discovered to be configured with default root credentials.	2024-02-02	9.8	CVE-2024-22902
vinchin -- vinchin_backup_and_recovery	Vinchin Backup & Recovery v7.2 was discovered to contain an authenticated remote code execution (RCE) vulnerability via the syncNtpTime function.	2024-02-02	8.8	CVE-2024-22899
vinchin -- vinchin_backup_and_recovery	Vinchin Backup & Recovery v7.2 was discovered to contain an authenticated remote code execution (RCE) vulnerability via the setNetworkCardInfo function.	2024-02-02	8.8	CVE-2024-22900
vinchin -- vinchin_backup_and_recovery	Vinchin Backup & Recovery v7.2 was discovered to contain an authenticated remote code execution (RCE) vulnerability via the deleteUpdateAPK function.	2024-02-02	8.8	CVE-2024-22903
vmware -- aria_operations_for_networks	Aria Operations for Networks contains a local privilege escalation vulnerability. A console user with access to Aria Operations for Networks may exploit this vulnerability to escalate privileges to gain root access to the system.	2024-02-06	7.8	CVE-2024-22237
vmware -- aria_operations_for_networks	Aria Operations for Networks contains a local privilege escalation vulnerability. A console user with access to Aria Operations for Networks may exploit this vulnerability to escalate privileges to gain regular shell access.	2024-02-06	7.8	CVE-2024-22239
vyper -- vyper	Vyper is a Pythonic Smart Contract Language for the Ethereum Virtual Machine. Arrays can be keyed by a signed integer, while they are defined for unsigned integers only. The typechecker doesn't throw when spotting the usage of an `int` as an index for an array. The typechecker allows the usage of signed integers to be used as indexes to arrays. The vulnerability is present in different forms in all versions, including `0.3.10`. For ints, the 2's complement representation is used. Because the array was declared very large, the bounds checking will pass Negative values will simply be represented as very large numbers. As of time of publication,	2024-02-07	9.8	CVE-2024-24563

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	a fixed version does not exist. There are three potential vulnerability classes: unpredictable behavior, accessing inaccessible elements and denial of service. Class 1: If it is possible to index an array with a negative integer without reverting, this is most likely not anticipated by the developer and such accesses can cause unpredictable behavior for the contract. Class 2: If a contract has an invariant in the form `assert index < x`, the developer will suppose that no elements on indexes `y | y >= x` are accessible. However, by using negative indexes, this can be bypassed. Class 3: If the index is dependent on the state of the contract, this poses a risk of denial of service. If the state of the contract can be manipulated in such way that the index will be forced to be negative, the array access can always revert (because most likely the array won't be declared extremely large). However, all these the scenarios are highly unlikely. Most likely behavior is a revert on the bounds check.			
westermo -- lynx	The cross-site request forgery token in the request may be predictable or easily guessable allowing attackers to craft a malicious request, which could be triggered by a victim unknowingly. In a successful CSRF attack, the attacker could lead the victim user to carry out an action unintentionally.	2024-02-06	8	CVE-2023-38579
westermo -- lynx	A potential attacker with access to the Westermo Lynx device may be able to execute malicious code that could affect the correct functioning of the device.	2024-02-06	8	CVE-2023-45735
wixtoolset -- issues	WiX toolset lets developers create installers for Windows Installer, the Windows installation engine. The .be TEMP folder is vulnerable to DLL redirection attacks that allow the attacker to escalate privileges. This impacts any installer built with the WiX installer framework. This issue has been patched in version 4.0.4.	2024-02-07	8.2	CVE-2024-24810
wordpress -- wordpress	The 3DPrint Lite WordPress plugin before 1.9.1.5 does not have any authorization and does not check the uploaded file in its p3dlite_handle_upload AJAX action, allowing unauthenticated users to upload arbitrary file to the web server. However, there is a .htaccess, preventing the file to be accessed on Web servers such as Apache.	2024-02-05	9.8	CVE-2021-4436
wordpress -- wordpress	The Better Search Replace plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.4.4 via deserialization of untrusted input. This makes it possible for unauthenticated attackers to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	2024-02-05	9.8	CVE-2023-6933
wordpress -- wordpress	The Shield Security - Smart Bot Blocking & Intrusion Prevention Security plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 18.5.9 via the render_action_template parameter. This makes it possible for unauthenticated attacker to include and execute PHP files on the server, allowing the execution of any PHP code in those files.	2024-02-05	9.8	CVE-2023-6989
wordpress -- wordpress	The Photo Gallery by 10Web - Mobile-Friendly Image Gallery plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.8.19 via the rename_item function. This makes it possible for authenticated attackers to rename arbitrary files on the server. This can lead to site takeovers if the wp-config.php file of a site can be renamed. By default, this can be exploited by administrators only. In the premium version of the plugin, administrators can give gallery management permissions to lower level users, which might make this exploitable by users as low as contributors.	2024-02-05	9.1	CVE-2024-0221
wordpress -- wordpress	The Ninja Forms Contact Form - The Drag and Drop Form Builder for WordPress plugin for WordPress is vulnerable to Second Order SQL Injection via the email address value submitted through forms in all versions up to, and including, 3.7.1 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 inject SQL in their email address that will append additional into the already existing query when an administrator triggers a personal data export.	2024-02-02	9.8	CVE-2024-0685
wordpress -- wordpress	The Cryptocurrency Widgets - Price Ticker & Coins List plugin for WordPress is vulnerable to SQL Injection via the 'coinslist' parameter in versions 2.0 to 2.6.5 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.	2024-02-05	9.8	CVE-2024-0709
wordpress -- wordpress	The WP Booking Calendar plugin for WordPress is vulnerable to SQL Injection via the 'calendar_request_params[dates_ddmmyy_csv]' parameter in all versions up to, and including, 9.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible	2024-02-08	9.8	CVE-2024-1207

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.			
wordpress -- wordpress	The Cookie Information | Free GDPR Consent Solution plugin for WordPress is vulnerable to arbitrary option updates due to a missing capability check on its AJAX request handler in versions up to, and including, 2.0.22. This makes it possible for authenticated attackers, with subscriber-level access or higher, to edit arbitrary site options which can be used to create administrator accounts.	2024-02-05	8.8	CVE-2023-6700
wordpress -- wordpress	The File Manager Pro plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 8.3.4 via the mk_check_filemanager_php_syntax AJAX function. This makes it possible for authenticated attackers, with subscriber access and above, to execute code on the server. Version 8.3.5 introduces a capability check that prevents users lower than admin from executing this function.	2024-02-05	8.8	CVE-2023-6846
wordpress -- wordpress	The Display custom fields in the frontend - Post and User Profile Fields plugin for WordPress is vulnerable to Code Injection via the plugin's vg_display_data shortcode in all versions up to, and including, 1.2.1 due to insufficient input validation and restriction on access to that shortcode. This makes it possible for authenticated attackers with contributor-level and above permissions to call arbitrary functions and execute code.	2024-02-05	8.8	CVE-2023-6996
wordpress -- wordpress	The User Profile Builder - Beautiful User Registration Forms, User Profiles & User Role Editor plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'wppb_two_factor_authentication_settings_update' function in all versions up to, and including, 3.10.8. This makes it possible for unauthenticated attackers to enable or disable the 2FA functionality present in the Premium version of the plugin for arbitrary user roles.	2024-02-05	8.2	CVE-2024-0324
wordpress -- wordpress	The Awesome Support - WordPress HelpDesk & Support Plugin plugin for WordPress is vulnerable to union-based SQL Injection via the 'q' parameter of the wpas_get_users action in all versions up to, and including, 6.1.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-02-10	8.8	CVE-2024-0594
wordpress -- wordpress	The File Manager plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 7.2.1 due to insufficient randomness in the backup filenames, which use a timestamp plus 4 random digits. This makes it possible for unauthenticated attackers, to extract sensitive data including site backups in configurations where the .htaccess file in the directory does not block access.	2024-02-05	8.1	CVE-2024-0761
wordpress -- wordpress	The Instant Images - One Click Image Uploads from Unsplash, Openverse, Pixabay and Pexels plugin for WordPress is vulnerable to unauthorized arbitrary options update due to an insufficient check that neglects to verify whether the updated option belongs to the plugin on the instant-images/license REST API endpoint in all versions up to, and including, 6.1.0. This makes it possible for authors and higher to update arbitrary options.	2024-02-05	8.8	CVE-2024-0869
wordpress -- wordpress	The Website Builder by SeedProd - Theme Builder, Landing Page Builder, Coming Soon Page, Maintenance Mode plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the seedprod_lite_new_lpage function in all versions up to, and including, 6.15.21. This makes it possible for unauthenticated attackers to change the contents of coming-soon, maintenance pages, login and 404 pages set up with the plugin. Version 6.15.22 addresses this issue but introduces a bug affecting admin pages. We suggest upgrading to 6.15.23.	2024-02-05	8.2	CVE-2024-1072
wordpress -- wordpress	The Podlove Subscribe button plugin for WordPress is vulnerable to UNION-based SQL Injection via the 'button' attribute of the podlove-subscribe-button shortcode in all versions up to, and including, 1.3.10 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-02-07	8.8	CVE-2024-1118
wordpress -- wordpress	The EditorsKit plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation on the 'import_styles' function in versions up to, and including, 1.40.3. This makes it possible for authenticated attackers with	2024-02-05	7.2	CVE-2023-6635

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	administrator-level capabilities or above, to upload arbitrary files on the affected site's server which may make remote code execution possible.			
wordpress -- wordpress	The Unlimited Addons for WPBakery Page Builder plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation on the 'importZipFile' function in versions up to, and including, 1.0.42. This makes it possible for authenticated attackers with a role that the administrator previously granted access to the plugin (the default is editor role, but access can also be granted to contributor role), to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-02-05	7.2	CVE-2023-6925
wordpress -- wordpress	The Index Now plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.6.3. This is due to missing or incorrect nonce validation on the 'reset_form' function. This makes it possible for unauthenticated attackers to delete arbitrary site options via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-02-05	7.1	CVE-2024-0428
wordpress -- wordpress	The Backuply - Backup, Restore, Migrate and Clone plugin for WordPress is vulnerable to Denial of Service in all versions up to, and including, 1.2.5. This is due to direct access of the backuply/restore_ins.php file and. This makes it possible for unauthenticated attackers to make excessive requests that result in the server running out of resources.	2024-02-09	7.5	CVE-2024-0842
wordpress -- wordpress	The Popup More Popups, Lightboxes, and more popup modules plugin for WordPress is vulnerable to Local File Inclusion in version 2.1.6 via the ycfChangeElementData() function. This makes it possible for authenticated attackers, with administrator-level access and above, to include and execute arbitrary files ending with "Form.php" on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included.	2024-02-02	7.2	CVE-2024-0844
wordpress -- wordpress	The Anonymous Restricted Content plugin for WordPress is vulnerable to information disclosure in all versions up to, and including, 1.6.2. This is due to insufficient restrictions through the REST API on the posts/pages that protections are being place on. This makes it possible for unauthenticated attackers to access protected content.	2024-02-03	7.5	CVE-2024-0909
wordpress -- wordpress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VeronaLabs WP SMS - Messaging & SMS Notification for WordPress, WooCommerce, GravityForms, etc allows Reflected XSS.This issue affects WP SMS - Messaging & SMS Notification for WordPress, WooCommerce, GravityForms, etc: from n/a through 6.5.2.	2024-02-08	7.1	CVE-2024-24881
xiandafu -- beetl	Before Beetl v3.15.12, the rendering template has a server-side template injection (SSTI) vulnerability. When the incoming template is controllable, it will be filtered by the DefaultNativeSecurityManager blacklist. Because blacklist filtering is not strict, the blacklist can be bypassed, leading to arbitrary code execution.	2024-02-02	9.8	CVE-2024-22533
xorg -- xorg-server	An out-of-bounds memory access flaw was found in the X.Org server. This issue can be triggered when a device frozen by a sync grab is reattached to a different master device. This issue may lead to an application crash, local privilege escalation (if the server runs with extended privileges), or remote code execution in SSH X11 forwarding environments.	2024-02-09	7.8	CVE-2024-0229
xxyopen -- novel-plus	A SQL injection vulnerability exists in Novel-Plus v4.3.0-RC1 and prior versions. An attacker can pass crafted offset, limit, and sort parameters to perform SQL injection via /novel/pay/list	2024-02-06	9.8	CVE-2024-24013
xxyopen -- novel-plus	A SQL injection vulnerability exists in Novel-Plus v4.3.0-RC1 and prior versions. An attacker can pass crafted offset, limit, and sort parameters to perform SQL injection via /novel/author/list	2024-02-08	9.8	CVE-2024-24014
xxyopen -- novel-plus	A SQL injection vulnerability exists in Novel-Plus v4.3.0-RC1 and prior versions. An attacker can pass in crafted offset, limit, and sort parameters to perform SQL via /sys/user/exit	2024-02-06	9.8	CVE-2024-24015

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xxyopen -- novel-plus	A SQL injection vulnerability exists in Novel-Plus v4.3.0-RC1 and prior versions. An attacker can pass crafted offset, limit, and sort parameters to perform SQL injection via /common/dict/list	2024-02-08	9.8	CVE-2024-24017
xxyopen -- novel-plus	A SQL injection vulnerability exists in Novel-Plus v4.3.0-RC1 and prior versions. An attacker can pass in crafted offset, limit, and sort parameters to perform SQL injection via /system/dataPerm/list	2024-02-08	9.8	CVE-2024-24018
xxyopen -- novel-plus	A SQL injection vulnerability exists in Novel-Plus v4.3.0-RC1 and prior versions. An attacker can pass in crafted offset, limit, and sort parameters to perform SQL injection via /system/roleDataPerm/list	2024-02-07	9.8	CVE-2024-24019
xxyopen -- novel-plus	A SQL injection vulnerability exists in Novel-Plus v4.3.0-RC1 and prior. An attacker can pass specially crafted offset, limit, and sort parameters to perform SQL injection via /novel/userFeedback/list.	2024-02-08	9.8	CVE-2024-24021
xxyopen -- novel-plus	A SQL injection vulnerability exists in Novel-Plus v4.3.0-RC1 and prior. An attacker can pass specially crafted offset, limit, and sort parameters to perform SQL injection via /novel/bookContent/list.	2024-02-08	9.8	CVE-2024-24023
xxyopen -- novel-plus	An arbitrary File download vulnerability exists in Novel-Plus v4.3.0-RC1 and prior at com.java2nb.common.controller.FileController: fileDownload(). An attacker can pass in specially crafted filePath and fieName parameters to perform arbitrary File download.	2024-02-08	9.8	CVE-2024-24024
xxyopen -- novel-plus	An arbitrary File upload vulnerability exists in Novel-Plus v4.3.0-RC1 and prior at com.java2nb.common.controller.FileController: upload(). An attacker can pass in specially crafted filename parameter to perform arbitrary File download.	2024-02-08	9.8	CVE-2024-24025
xxyopen -- novel-plus	An arbitrary File upload vulnerability exists in Novel-Plus v4.3.0-RC1 and prior versions at com.java2nb.system.controller.SysUserController: uploadImg(). An attacker can pass in specially crafted filename parameter to perform arbitrary File download.	2024-02-08	9.8	CVE-2024-24026
yannick_lefebvre -- link_library	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Yannick Lefebvre Link Library allows Reflected XSS. This issue affects Link Library: from n/a through 7.5.13.	2024-02-08	7.1	CVE-2024-24879
yarn -- yarn	An untrusted search path vulnerability was found in Yarn. When a victim runs certain Yarn commands in a directory with attacker-controlled content, malicious commands could be executed in unexpected ways.	2024-02-04	7.7	CVE-2021-4435
zohocorp -- manageengine_adaudit_plus	Zoho ManageEngine ADAudit Plus through 7250 is vulnerable to SQL Injection in the report export option.	2024-02-02	9.8	CVE-2023-48792
zohocorp -- manageengine_adaudit_plus	Zoho ManageEngine ADAudit Plus through 7250 allows SQL Injection in the aggregate report feature.	2024-02-02	9.8	CVE-2023-48793
zohocorp -- manageengine_adaudit_plus	ManageEngine ADAudit Plus versions 7270 and below are vulnerable to the Authenticated SQL injection in home Graph-Data.	2024-02-02	8.8	CVE-2024-0253
zohocorp -- manageengine_adaudit_plus	ManageEngine ADAudit Plus versions 7270 and below are vulnerable to the Authenticated SQL injection in File-Summary DrillDown. This issue has been fixed and released in version 7271.	2024-02-02	8.8	CVE-2024-0269
zopefoundation -- products_sqlalchemyda	SQLAlchemyDA is a generic database adapter for ZSQL methods. A vulnerability found in versions prior to 2.2 allows unauthenticated execution of arbitrary SQL statements on the database to which the SQLAlchemyDA instance is connected. All users are affected. The problem has been patched in version 2.2. There is no workaround for the problem.	2024-02-07	9.8	CVE-2024-24811

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- commons_compress	Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in Apache Commons Compress.This issue affects Apache Commons Compress: from 1.3 through 1.25.0. Users are recommended to upgrade to version 1.26.0 which fixes the issue.	2024-02-19	5.5	CVE-2024-25710

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- commons_compress	Allocation of Resources Without Limits or Throttling vulnerability in Apache Commons Compress.This issue affects Apache Commons Compress: from 1.21 before 1.26. Users are recommended to upgrade to version 1.26, which fixes the issue.	2024-02-19	5.5	CVE-2024-26308
apostrophe -- sanitize-html	Versions of the package sanitize-html before 2.12.1 are vulnerable to Information Exposure when used on the backend and with the style attribute allowed, allowing enumeration of files in the system (including project dependencies). An attacker could exploit this vulnerability to gather details about the file system structure and dependencies of the targeted server.	2024-02-24	5.3	CVE-2024-21501
archer -- archer_platform	Archer Platform 6.x before 6.14 P2 HF1 (6.14.0.2.1) contains a reflected XSS vulnerability. A remote authenticated malicious Archer user could potentially exploit this by tricking a victim application user into supplying malicious JavaScript code to the vulnerable web application. This code is then reflected to the victim and gets executed by the web browser in the context of the vulnerable web application.	2024-02-21	5.7	CVE-2024-26311
archer -- archer_platform	Denial of service condition in M-Files Server inversions before 24.2 (excluding 23.2 SR7 and 23.8 SR5) allows anonymous user to cause denial of service against other anonymous users.	2024-02-23	4.3	CVE-2024-0563
archer -- platform	Archer Platform 6.8 before 6.14 P2 (6.14.0.2) contains an improper access control vulnerability. A remote authenticated malicious user could potentially exploit this to gain access to API information that should only be accessible with extra privileges.	2024-02-21	4.3	CVE-2024-26310
arne_franken -- all_in_one_favicon	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Arne Franken All In One Favicon.This issue affects All In One Favicon: from n/a through 4.7.	2024-02-23	6.8	CVE-2023-24416
baserproject -- basercms	baserCMS is a website development framework. Prior to version 5.0.9, there is a cross-site scripting vulnerability in the content management feature. Version 5.0.9 contains a fix for this vulnerability.	2024-02-22	5.4	CVE-2024-26128
baserproject -- basercms	baserCMS is a website development framework. Prior to version 5.0.9, there is a cross-site scripting vulnerability in the site search feature. Version 5.0.9 contains a fix for this vulnerability.	2024-02-22	6.1	CVE-2023-44379
baserproject -- basercms	baserCMS is a website development framework. Prior to version 5.0.9, there is an OS Command Injection vulnerability in the site search feature of baserCMS. Version 5.0.9 contains a fix for this vulnerability.	2024-02-22	5.6	CVE-2023-51450
c-ares -- c-ares	c-ares is a C library for asynchronous DNS requests. `ares__read_line()` is used to parse local configuration files such as `/etc/resolv.conf`, `/etc/nsswitch.conf`, the `HOSTALIASES` file, and if using a c-ares version prior to 1.27.0, the `/etc/hosts` file. If any of these configuration files has an embedded `NULL` character as the first character in a new line, it can lead to attempting to read memory prior to the start of the given buffer which may result in a crash. This issue is fixed in c-ares 1.27.0. No known workarounds exist.	2024-02-23	4.4	CVE-2024-25629
cilium -- cilium	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. For Cilium users who are using CRDs to store Cilium state (the default configuration) and Wireguard transparent encryption, traffic to/from the Ingress and health endpoints is not encrypted. This issue affects Cilium v1.14 before v1.14.7 and has been patched in Cilium v1.14.7. There is no workaround to this issue.	2024-02-20	6.1	CVE-2024-25630
cilium -- cilium	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. For Cilium users who have enabled an external kvstore and Wireguard transparent encryption, traffic between pods in the affected cluster is not	2024-02-20	6.1	CVE-2024-25631

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	encrypted. This issue affects Cilium v1.14 before v1.14.7 and has been patched in Cilium v1.14.7. There is no workaround to this issue.			
cisco -- cisco_unified_intelligence_center	A vulnerability in the Live Data server of Cisco Unified Intelligence Center could allow an unauthenticated, local attacker to read and modify data in a repository that belongs to an internal service on an affected device. This vulnerability is due to insufficient access control implementations on cluster configuration CLI requests. An attacker could exploit this vulnerability by sending a cluster configuration CLI request to specific directories on an affected device. A successful exploit could allow the attacker to read and modify data that is handled by an internal service on the affected device.	2024-02-21	5.1	CVE-2024-20325
code-projects -- crime_reporting_system	A vulnerability was found in code-projects Crime Reporting System 1.0. It has been rated as critical. This issue affects some unknown processing of the file police_add.php. The manipulation of the argument police_name/police_id/police_spec/password leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-254609 was assigned to this vulnerability.	2024-02-23	5.5	CVE-2024-1821
codeastro -- simple_voting_system	A vulnerability classified as critical was found in CodeAstro Simple Voting System 1.0. Affected by this vulnerability is an unknown functionality of the file users.php of the component Backend. 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-254611.	2024-02-23	5.3	CVE-2024-1823
codeastro -- house_rental_management_system	A vulnerability, which was classified as problematic, was found in CodeAstro House Rental Management System 1.0. This affects an unknown part of the component User Registration Page. The manipulation of the argument address with the input <img src="1" onerror="console.log(1)"> 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-254613 was assigned to this vulnerability.	2024-02-23	4.3	CVE-2024-1825
codeastro -- membership_management_system	A vulnerability was found in CodeAstro Membership Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /uploads/ of the component Logo Handler. The manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-254606 is the identifier assigned to this vulnerability.	2024-02-23	4.7	CVE-2024-1818
codeastro -- membership_management_system	A vulnerability was found in CodeAstro Membership Management System 1.0. It has been classified as critical. This affects an unknown part of the component Add Members Tab. The manipulation of the argument Member Photo leads to unrestricted upload. 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-254607.	2024-02-23	4.7	CVE-2024-1819
david_stockl -- tinymce_and_tinymce_advanced_professional_formats_and_styles	Cross-Site Request Forgery (CSRF) vulnerability in David Stockl TinyMCE and TinyMCE Advanced Professsional Formats and Styles.This issue affects TinyMCE and TinyMCE Advanced Professsional Formats and Styles: from n/a through 1.1.2.	2024-02-21	4.3	CVE-2024-25904
decidim -- decidim	Decidim is a participatory democracy framework. Starting in version 0.23.0 and prior to versions 0.27.5 and 0.28.0, the CSRF authenticity token check is disabled for the questionnaire templates preview. The issue does not imply a serious security thread as you need to have access also to the session cookie in order to see this resource. This URL does not allow modifying the resource but it may allow attackers to gain access to information which was not meant to be public. The issue is fixed in version 0.27.5 and 0.28.0. As a workaround, disable the templates functionality or remove all available templates.	2024-02-20	4.5	CVE-2023-47635

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
decidim -- decidim	Decidim is a participatory democracy framework. Starting in version 0.27.0 and prior to versions 0.27.5 and 0.28.0, the dynamic file upload feature is subject to potential cross-site scripting attacks in case the attacker manages to modify the file names of the records being uploaded to the server. This appears in sections where the user controls the file upload dialogs themselves and has the technical knowledge to change the file names through the dynamic upload endpoint. Therefore I believe it would require the attacker to control the whole session of the particular user but in any case, this needs to be fixed. Successful exploit of this vulnerability would require the user to have successfully uploaded a file blob to the server with a malicious file name and then have the possibility to direct the other user to the edit page of the record where the attachment is attached. The users are able to craft the direct upload requests themselves controlling the file name that gets stored to the database. The attacker is able to change the filename e.g. to `<svg onload=alert('XSS')>` if they know how to craft these requests themselves. And then enter the returned blob ID to the form inputs manually by modifying the edit page source. Versions 0.27.5 and 0.28.0 contain a patch for this issue. As a workaround, disable dynamic uploads for the instance, e.g. from proposals.	2024-02-20	6.3	CVE-2023-51447
decidim -- decidim	Decidim is a participatory democracy framework. Starting in version 0.4.rc3 and prior to version 2.0.9 of the `devise_invitable` gem, the invites feature allows users to accept the invitation for an unlimited amount of time through the password reset functionality. This issue creates vulnerable dependencies starting in version 0.0.1.alpha3 and prior to versions 0.26.9, 0.27.5, and 0.28.0 of the `decidim,` `decidim-admin`, and `decidim-system` gems. When using the password reset functionality, the `devise_invitable` gem always accepts the pending invitation if the user has been invited. The only check done is if the user has been invited but the code does not ensure that the pending invitation is still valid as defined by the `invite_for` expiry period. Decidim sets this configuration to `2.weeks` so this configuration should be respected. The bug is in the `devise_invitable` gem and should be fixed there and the dependency should be upgraded in Decidim once the fix becomes available. `devise_invitable` to version `2.0.9` and above fix this issue. Versions 0.26.9, 0.27.5, and 0.28.0 of the `decidim,` `decidim-admin`, and `decidim-system` gems contain this fix. As a workaround, invitations can be cancelled directly from the database.	2024-02-20	5.7	CVE-2023-48220
desertsnowman -- plugin_groups	The Plugin Groups plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the admin_init() function in all versions up to, and including, 2.0.6. This makes it possible for unauthenticated attackers to change the settings of the plugin, which can also cause a denial of service due to a misconfiguration.	2024-02-21	6.5	CVE-2024-1108
dfir-iris -- iris-web	Iris is a web collaborative platform that helps incident responders share technical details during investigations. A stored Cross-Site Scripting (XSS) vulnerability has been identified in iris-web, affecting multiple locations in versions prior to v2.4.0. The vulnerability may allow an attacker to inject malicious scripts into the application, which could then be executed when a user visits the affected locations. This could lead to unauthorized access, data theft, or other related malicious activities. An attacker need to be authenticated on the application to exploit this vulnerability. The issue is fixed in version v2.4.0 of iris-web. No workarounds are available.	2024-02-19	4.6	CVE-2024-25640
discourse -- discourse-calendar	Discourse Calendar adds the ability to create a dynamic calendar in the first post of a topic on the open-source discussion platform Discourse. Prior to version 0.4, event invitees created in topics in private categories or PMs (private messages) can be retrieved by anyone, even if they're not logged in. This problem is resolved in version 0.4 of the discourse-calendar plugin. While no known workaround is available, putting the site behind `login_required` will disallow this endpoint to be used by anonymous users, but logged in users can still get the list of invitees in the private topics.	2024-02-22	4.3	CVE-2024-24817

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
discourse -- discourse-calendar	Discourse Calendar adds the ability to create a dynamic calendar in the first post of a topic on Discourse. Uninvited users are able to gain access to private events by crafting a request to update their attendance. This problem is resolved in commit dfc4fa15f340189f177a1d1ab2cc94ffed3c1190. As a workaround, one may use post visibility to limit access.	2024-02-21	6.5	CVE-2024-26145
discourse-- discourse-ai	discourse-ai is the AI plugin for the open-source discussion platform Discourse. Prior to commit 94ba0dadc2cf38e8f81c3936974c167219878edd, interactions with different AI services are vulnerable to admin-initiated SSRF attacks. Versions of the plugin that include commit 94ba0dadc2cf38e8f81c3936974c167219878edd contain a patch. As a workaround, one may disable the discourse-ai plugin.	2024-02-21	4.1	CVE-2024-23654
dompdf -- php-svg-lib	php-svg-lib is a scalable vector graphics (SVG) file parsing/rendering library. Prior to version 0.5.2, php-svg-lib fails to validate that font-family doesn't contain a PHAR url, which might leads to RCE on PHP < 8.0, and doesn't validate if external references are allowed. This might leads to bypass of restrictions or RCE on projects that are using it, if they do not strictly revalidate the fontName that is passed by php-svg-lib. The `Style::fromAttributes(`), or the `Style::parseCssStyle()` should check the content of the `font-family` and prevents it to use a PHAR url, to avoid passing an invalid and dangerous `fontName` value to other libraries. The same check as done in the `Style::fromStyleSheets` might be reused. Libraries using this library as a dependency might be vulnerable to some bypass of restrictions, or even remote code execution, if they do not double check the value of the `fontName` that is passed by php-svg-lib. Version 0.5.2 contains a fix for this issue.	2024-02-21	6.8	CVE-2024-25117
enalean -- tuleap	Tuleap is an open source suite to improve management of software developments and collaboration. Prior to version 15.5.99.76 of Tuleap Community Edition and prior to versions 15.5-4 and 15.4-7 of Tuleap Enterprise Edition, users with a read access to a tracker where the mass update feature is used might get access to restricted information. Tuleap Community Edition 15.5.99.76, Tuleap Enterprise Edition 15.5-4, and Tuleap Enterprise Edition 15.4-7 contain a patch for this issue.	2024-02-22	5.4	CVE-2024-25130
eteubert -- archivist_-_custom_archive_templates	The Archivist - Custom Archive Templates plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'shortcode_attributes' parameter in all versions up to, and including, 1.7.5 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.	2024-02-24	6.1	CVE-2024-1810
eventstore -- eventstore	EventStoreDB (ESDB) is an operational database built to store events. A vulnerability has been identified in the projections subsystem in versions 20 prior to 20.10.6, 21 prior to 21.10.11, 22 prior to 22.10.5, and 23 prior to 23.10.1. Only database instances that use custom projections are affected by this vulnerability. User passwords may become accessible to those who have access to the chunk files on disk, and users who have read access to system streams. Only users in the `$admins` group can access system streams by default. ESDB 23.10.1, 22.10.5, 21.10.11, and 20.10.6 contain a patch for this issue. Users should upgrade EventStoreDB, reset the passwords for current and previous members of `$admins` and `$ops` groups, and, if a password was reused in any other system, reset it in those systems to a unique password to follow best practices. If an upgrade cannot be done immediately, reset the passwords for current and previous members of `$admins` and `$ops` groups. Avoid creating custom projections until the patch has been applied.	2024-02-21	5.5	CVE-2024-26133
extendthemes -- colibri_page_builder	The Colibri WP theme for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.94. This is due to missing or incorrect nonce validation on the colibriwp_install_plugin() function. This makes it possible for unauthenticated attackers to install recommended plugins via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-02-23	4.3	CVE-2024-1360

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
extendthemes -- colibri_page_builder	The Colibri Page Builder plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.253. This is due to missing or incorrect nonce validation on the apiCall() function. This makes it possible for unauthenticated attackers to call a limited set of functions that can be used to import images, delete posts, or save theme data via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-02-23	4.3	CVE-2024-1361
extendthemes -- colibri_page_builder	The Colibri Page Builder plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.253. This is due to missing or incorrect nonce validation on the cp_shortcode_refresh() function. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-02-23	4.3	CVE-2024-1362
fortinet -- fortiproxy	A null pointer dereference in Fortinet FortiOS version 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.12, Fortiproxy version 7.2.0 through 7.2.4, 7.0.0 through 7.0.10 allows attacker to denial of service via specially crafted HTTP requests.	2024-02-22	6.5	CVE-2023-29179
frederic_gilles -- fg_prestashop_to_woocommerce	Cross-Site Request Forgery (CSRF) vulnerability in Frederic GILLES FG PrestaShop to WooCommerce, Frederic GILLES FG Drupal to WordPress, Frederic GILLES FG Joomla to WordPress.This issue affects FG PrestaShop to WooCommerce: from n/a through 4.44.3; FG Drupal to WordPress: from n/a through 3.67.0; FG Joomla to WordPress: from n/a through 4.15.0.	2024-02-21	4.3	CVE-2024-24837
garo -- wallbox_glb+_t2ev7	A vulnerability, which was classified as problematic, was found in GARO WALLBOX GLB+ T2EV7 0.5. This affects an unknown part of the file /index.jsp#settings of the component Software Update Handler. The manipulation of the argument Reference 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-254397 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-21	4.3	CVE-2024-1707
gitlab -- gitlab	An issue has been discovered in GitLab EE affecting all versions starting from 12.0 to 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. This vulnerability allows for bypassing the 'group ip restriction' settings to access environment details of projects	2024-02-22	4.3	CVE-2023-4895
gitlab -- gitlab	An issue has been discovered in GitLab EE affecting all versions starting from 16.5 before 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. When a user is assigned a custom role with admin_group_member permission, they may be able to make a group, other members or themselves Owners of that group, which may lead to privilege escalation.	2024-02-22	6.7	CVE-2023-6477
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.1 before 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. Under some specialized conditions, an LDAP user may be able to reset their password using their verified secondary email address and sign-in using direct authentication with the reset password, bypassing LDAP.	2024-02-22	5.3	CVE-2024-1525
gitlab --gitlab	An issue has been discovered in GitLab EE affecting all versions starting from 16.4 before 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. Users with the `Guest` role can change `Custom dashboard projects` settings contrary to permissions.	2024-02-22	4.3	CVE-2024-0861
gn_themes -- wp_shortcodes_plugin_-_shortcodes_ultimate	The WP Shortcodes Plugin - Shortcodes Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's su_tooltip shortcode in all versions up to, and including, 7.0.2 due to insufficient input sanitization and output escaping on user supplied attributes and user supplied tags. This makes it possible for authenticated attackers with contributor-level and above permissions to inject	2024-02-20	6.4	CVE-2024-1510

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
greenpau -- github.com/greenpau/caddy-security	All versions of the package github.com/greenpau/caddy-security are vulnerable to Insufficient Session Expiration due to improper user session invalidation upon clicking the "Sign Out" button. User sessions remain valid even after requests are sent to /logout and /oauth2/google/logout. Attackers who gain access to an active but supposedly logged-out session can perform unauthorized actions on behalf of the user.	2024-02-17	4.8	CVE-2024-21492
greenpau -- github.com/greenpau/caddy-security	All versions of the package github.com/greenpau/caddy-security are vulnerable to HTTP Header Injection via the X-Forwarded-Proto header due to redirecting to the injected protocol.Exploiting this vulnerability could lead to bypass of security mechanisms or confusion in handling TLS.	2024-02-17	4.3	CVE-2024-21499
greenpau -- github.com/greenpau/caddy-security	All versions of the package github.com/greenpau/caddy-security are vulnerable to Improper Restriction of Excessive Authentication Attempts via the two-factor authentication (2FA). Although the application blocks the user after several failed attempts to provide 2FA codes, attackers can bypass this blocking mechanism by automating the application's full multistep 2FA process.	2024-02-17	4.8	CVE-2024-21500
greenpau -- github.com/greenpau/caddy-security	All versions of the package github.com/greenpau/caddy-security are vulnerable to Improper Validation of Array Index when parsing a Caddyfile. Multiple parsing functions in the affected library do not validate whether their input values are nil before attempting to access elements, which can lead to a panic (index out of range). Panics during the parsing of a configuration file may introduce ambiguity and vulnerabilities, hindering the correct interpretation and configuration of the web server.	2024-02-17	5.3	CVE-2024-21493
greenpau -- github.com/greenpau/caddy-security	All versions of the package github.com/greenpau/caddy-security are vulnerable to Authentication Bypass by Spoofing via the X-Forwarded-For header due to improper input sanitization. An attacker can spoof an IP address used in the user identity module (/whoami API endpoint). This could lead to unauthorized access if the system trusts this spoofed IP address.	2024-02-17	5.4	CVE-2024-21494
greenpau -- github.com/greenpau/caddy-security	All versions of the package github.com/greenpau/caddy-security are vulnerable to Open Redirect via the redirect_url parameter. An attacker could perform a phishing attack and trick users into visiting a malicious website by crafting a convincing URL with this parameter. To exploit this vulnerability, the user must take an action, such as clicking on a portal button or using the browser's back button, to trigger the redirection.	2024-02-17	5.4	CVE-2024-21497
greenpau -- github.com/greenpau/caddy-security	All versions of the package github.com/greenpau/caddy-security are vulnerable to Server-side Request Forgery (SSRF) via X-Forwarded-Host header manipulation. An attacker can expose sensitive information, interact with internal services, or exploit other vulnerabilities within the network by exploiting this vulnerability.	2024-02-17	5.3	CVE-2024-21498
humansignal -- label-studio	### Summary On all Label Studio versions prior to 1.11.0, data imported via file upload feature is not properly sanitized prior to being rendered within a [`Choices`](https://labelstud.io/tags/choices) or [`Labels`](https://labelstud.io/tags/labels) tag, resulting in an XSS vulnerability. ### Details Need permission to use the "data import" function. This was reproduced on Label Studio 1.10.1. ### PoC 1. Create a project. ![Create a project](https://github.com/HumanSignal/label-studio/assets/3943358/9b1536ad-feac-4238-a1bd-ca9b1b798673) 2. Upload a file containing the payload using the "Upload Files" function. ![2 Upload a file containing the payload using the Upload Files function](https://github.com/HumanSignal/label-studio/assets/3943358/26bb7af1-1cd2-408f-9adf-61e31a5b7328) ![3 complete](https://github.com/HumanSignal/label-studio/assets/3943358/f2f62774-1fa6-4456-9e6f-8fa1ca0a2d2e) The following are the contents of the files used in the PoC ``` { "data": { "prompt": "labelstudio	2024-02-22	4.7	CVE-2024-26152

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	universe image", "images": [{ "value": "id123#0", "style": "margin: 5px", "html": "<img width='400' src='https://labelstud.io/_astro/images-tab.64279c16_ZaBSvC.avif' onload=alert(document.cookie)>" }] } } ``` 3. Select the text-to-image generation labeling template of Ranking and scoring ![3 Select the text-to-image generation labelling template for Ranking and scoring](https://github.com/HumanSignal/label-studio/assets/3943358/f227f49c-a718-4738-bc2a-807da4f97155) ![5 save](https://github.com/HumanSignal/label-studio/assets/3943358/9b529f8a-8e99-4bb0-bdf6-bb7a95c9b75d) 4. Select a task ![4 Select a task](https://github.com/HumanSignal/label-studio/assets/3943358/71856b7a-2b1f-44ea-99ab-fc48bc20caa7) 5. Check that the script is running ![5 Check that the script is running](https://github.com/HumanSignal/label-studio/assets/3943358/e396ae7b-a591-4db7-afe9-5bab30b48cb9) ### Impact Malicious scripts can be injected into the code, and when linked with vulnerabilities such as CSRF, it can cause even greater damage. In particular, It can become a source of further attacks, especially when linked to social engineering.			
iberezansky -- 3d_flipbook_-_pdf_flipbook_wordpress	The 3D FlipBook - PDF Flipbook WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's bookmark feature in all versions up to, and including, 1.15.3 due to insufficient input sanitization and output escaping. 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.	2024-02-21	6.4	CVE-2024-1081
ibm -- common_licensing	IBM Common Licensing 9.0 could allow a local user to enumerate usernames due to an observable response discrepancy. IBM X-Force ID: 273337.	2024-02-20	4	CVE-2023-50306
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 256544.	2024-02-21	5.4	CVE-2023-33843
ibm -- qradar_suite_software	IBM QRadar Suite 1.10.12.0 through 1.10.17.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 in some circumstances will log some sensitive information about invalid authorization attempts. IBM X-Force ID: 275747.	2024-02-17	4	CVE-2023-50951
ibm -- qradar_suite_software	IBM QRadar Suite 1.10.12.0 through 1.10.17.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 279975.	2024-02-17	5.1	CVE-2024-22335
ibm -- qradar_suite_software	IBM QRadar Suite 1.10.12.0 through 1.10.17.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 279976.	2024-02-17	5.1	CVE-2024-22336
ibm -- qradar_suite_software	IBM QRadar Suite 1.10.12.0 through 1.10.17.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 279977.	2024-02-17	5.1	CVE-2024-22337
jackdewey -- link_library	The Link Library plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'll_reciprocal' parameter in all versions up to, and including, 7.6 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.	2024-02-20	6.5	CVE-2024-1559
janis_elsts -- admin_menu_editor	Cross-Site Request Forgery (CSRF) vulnerability in Janis Elsts Admin Menu Editor.This issue affects Admin Menu Editor: from n/a through 1.12.	2024-02-21	4.3	CVE-2024-24876
john_tendik -- jtrt_responsive_tables	Cross-Site Request Forgery (CSRF) vulnerability in John Tendik JTRT Responsive Tables.This issue affects JTRT Responsive Tables: from n/a through 4.1.9.	2024-02-21	4.3	CVE-2024-24802

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jumpserver -- jumpserver	JumpServer is an open source bastion host and an operation and maintenance security audit system. Prior to version 3.10.0, attackers can exploit this vulnerability to construct malicious links, leading users to click on them, thereby facilitating phishing attacks or cross-site scripting attacks. Version 3.10.0 contains a patch for this issue. No known workarounds are available.	2024-02-20	4.3	CVE-2024-24763
keerti1924 -- php-mysql-user-login-system	A vulnerability, which was classified as problematic, was found in keerti1924 PHP-MYSQL-User-Login-System 1.0. Affected is an unknown function of the file /signup.php. The manipulation of the argument username with the input <script>alert("xss")</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-254388. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-21	4.3	CVE-2024-1700
keerti1924 -- php-mysql-user-login-system	A vulnerability was found in keerti1924 PHP-MYSQL-User-Login-System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /edit.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-254390 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-21	6.3	CVE-2024-1702
keerti1924 -- php-mysql-user-login-system	A vulnerability has been found in keerti1924 PHP-MYSQL-User-Login-System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /edit.php. 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 identifier VDB-254389 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-21	5.3	CVE-2024-1701
laborofficefree -- laborofficefree	A weak permission was found in the backup directory in LaborOfficeFree affecting version 19.10. This vulnerability allows any authenticated user to read backup files in the directory '%programfiles(x86)% LaborOfficeFree BackUp'.	2024-02-19	4.7	CVE-2024-1343
laborofficefree_ -- laborofficefree_	Encrypted database credentials in LaborOfficeFree affecting version 19.10. This vulnerability allows an attacker to read and extract the username and password from the database of 'LOF_service.exe' and 'LaborOfficeFree.exe' located in the '%programfiles(x86)%\LaborOfficeFree\' directory. This user can log in remotely and has root-like privileges.	2024-02-19	6.8	CVE-2024-1344
laborofficefree_ -- laborofficefree_	Weak MySQL database root password in LaborOfficeFree affects version 19.10. This vulnerability allows an attacker to perform a brute force attack and easily discover the root password.	2024-02-19	6.8	CVE-2024-1345
laborofficefree_ -- laborofficefree_	Weak MySQL database root password in LaborOfficeFree affects version 19.10. This vulnerability allows an attacker to calculate the root password of the MySQL database used by LaborOfficeFree using two constants.	2024-02-19	6.8	CVE-2024-1346
liferay -- dxp	Open redirect vulnerability in adaptive media administration page in Liferay DXP 2023.Q3 before patch 6, and 7.4 GA through update 92 allows remote attackers to redirect users to arbitrary external URLs via the _com_liferay_adaptive_media_web_portlet_AMPortlet_redirect parameter.	2024-02-20	6.1	CVE-2023-44308
liferay -- portal	Information disclosure vulnerability in the Control Panel in Liferay Portal 7.2.0 through 7.4.2, and older unsupported versions, and Liferay DXP 7.3 before update 4, 7.2 before fix pack 19, and older unsupported versions allows remote authenticated users to obtain a user's full name from the page's title by enumerating user screen names.	2024-02-20	4.3	CVE-2024-25150
liferay -- portal	Open redirect vulnerability in the Countries Management's edit region page in Liferay Portal 7.4.3.45 through 7.4.3.101, and Liferay DXP 2023.Q3 before patch 6, and 7.4 update 45 through 92 allows remote attackers to redirect users to arbitrary external URLs via the	2024-02-20	6.1	CVE-2023-5190

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	_com_liferay_address_web_internal_portlet_CountriesManagementAdminPortlet _redirect parameter.			
liferay -- portal	Liferay Portal 7.2.0 through 7.4.3.4, and older unsupported versions, and Liferay DXP 7.4.13, 7.3 before service pack 3, 7.2 before fix pack 17, and older unsupported versions does not properly check user permissions, which allows remote authenticated users with the VIEW user permission to edit their own permission via the User and Organizations section of the Control Panel.	2024-02-20	6.5	CVE-2024-25604
liferay -- portal	HtmlUtil.escapeRedirect in Liferay Portal 7.2.0 through 7.4.3.18, and older unsupported versions, and Liferay DXP 7.4 before update 19, 7.3 before update 4, 7.2 before fix pack 19, and older unsupported versions can be circumvented by using the 'REPLACEMENT CHARACTER' (U+FFFD), which allows remote attackers to redirect users to arbitrary external URLs via the (1) 'redirect` parameter (2) `FORWARD_URL` parameter, (3) `noSuchEntryRedirect` parameter, and (4) others parameters that rely on HtmlUtil.escapeRedirect.	2024-02-20	6.1	CVE-2024-25608
liferay -- portal	HtmlUtil.escapeRedirect in Liferay Portal 7.2.0 through 7.4.3.12, and older unsupported versions, and Liferay DXP 7.4 before update 9, 7.3 service pack 3, 7.2 fix pack 15 through 18, and older unsupported versions can be circumvented by using two forward slashes, which allows remote attackers to redirect users to arbitrary external URLs via the (1) 'redirect` parameter (2) `FORWARD_URL` parameter, and (3) others parameters that rely on HtmlUtil.escapeRedirect. This vulnerability is the result of an incomplete fix in CVE-2022-28977.	2024-02-20	6.1	CVE-2024-25609
liferay -- portal	The Account Settings page in Liferay Portal 7.4.3.76 through 7.4.3.99, and Liferay DXP 2023.Q3 before patch 5, and 7.4 update 76 through 92 embeds the user's hashed password in the page's HTML source, which allows man-in-the-middle attackers to steal a user's hashed password.	2024-02-20	6.5	CVE-2024-26270
liferay -- portal	Liferay Portal 7.2.0 through 7.4.1, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 15, and older unsupported versions does not properly restrict membership of a child site when the "Limit membership to members of the parent site" option is enabled, which allows remote authenticated users to add users who are not a member of the parent site to a child site. The added user may obtain permission to perform unauthorized actions in the child site.	2024-02-20	5.4	CVE-2024-25149
liferay -- portal	The Image Uploader module in Liferay Portal 7.2.0 through 7.4.3.15, and older unsupported versions, and Liferay DXP 7.4 before update 16, 7.3 before update 4, 7.2 before fix pack 19, and older unsupported versions relies on a request parameter to limit the size of files that can be uploaded, which allows remote authenticated users to upload arbitrarily large files to the system's temp folder by modifying the `maxFileSize` parameter.	2024-02-20	5	CVE-2024-26265
liferay -- portal_	In Liferay Portal 7.2.0 through 7.4.3.25, and older unsupported versions, and Liferay DXP 7.4 before update 26, 7.3 before update 5, 7.2 before fix pack 19, and older unsupported versions the default value of the portal property `http.header.version.verbosity` is set to `full`, which allows remote attackers to easily identify the version of the application that is running and the vulnerabilities that affect that version via 'Liferay-Portal` response header.	2024-02-20	5.3	CVE-2024-26267
liferay -- portal	User enumeration vulnerability in Liferay Portal 7.2.0 through 7.4.3.26, and older unsupported versions, and Liferay DXP 7.4 before update 27, 7.3 before update 8, 7.2 before fix pack 20, and older unsupported versions allows remote attackers to determine if an account exist in the application by comparing the request's response time.	2024-02-20	5.3	CVE-2024-26268
liferay -- portal	The Calendar module in Liferay Portal 7.2.0 through 7.4.2, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 15, and older unsupported versions does not escape user supplied data in the default notification email template, which allows remote authenticated users to inject	2024-02-21	5.4	CVE-2024-25151

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary web script or HTML via the title of a calendar event or the user's name. This may lead to a content spoofing or cross-site scripting (XSS) attacks depending on the capability of the receiver's mail client.			
liferay -- portal	The Journal module in Liferay Portal 7.2.0 through 7.4.3.4, and older unsupported versions, and Liferay DXP 7.4.13, 7.3 before service pack 3, 7.2 before fix pack 17, and older unsupported versions grants guest users view permission to web content templates by default, which allows remote attackers to view any template via the UI or API.	2024-02-20	5.3	CVE-2024-25605
mark_stockton -- quicksand_post_filter_jquery_plugin	Cross-Site Request Forgery (CSRF) vulnerability in Mark Stockton Quicksand Post Filter jQuery Plugin. This issue affects Quicksand Post Filter jQuery Plugin: from n/a through 3.1.1.	2024-02-21	4.3	CVE-2024-24849
microsoft -- microsoft_edge	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	2024-02-23	4.8	CVE-2024-21423
microsoft -- microsoft_edge_for_adroid	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-02-23	4.3	CVE-2024-26188
mondula_gmbh -- multi_step_form	Cross-Site Request Forgery (CSRF) vulnerability in Mondula GmbH Multi Step Form.This issue affects Multi Step Form: from n/a through 1.7.18.	2024-02-21	5.4	CVE-2024-25905
moodle -- moodle	Separate Groups mode restrictions were not honored in the H5P attempts report, which would display users from other groups. By default this only provided additional access to non-editing teachers.	2024-02-19	4.3	CVE-2024-25980
moodle -- moodle	Separate Groups mode restrictions were not honored when performing a forum export, which would export forum data for all groups. By default this only provided additional access to non-editing teachers.	2024-02-19	4.3	CVE-2024-25981
moodle -- moodle	The link to update all installed language packs did not include the necessary token to prevent a CSRF risk.	2024-02-19	4.3	CVE-2024-25982
moodle -- moodle	The URL parameters accepted by forum search were not limited to the allowed parameters.	2024-02-19	5.3	CVE-2024-25979
netapp -- snapcenter	SnapCenter versions 4.8 prior to 5.0 are susceptible to a vulnerability which could allow an authenticated SnapCenter Server user to modify system logging configuration settings	2024-02-16	5.4	CVE-2024-21987
netapp -- storagegrid	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.8 are susceptible to a difficult to exploit Reflected Cross-Site Scripting (XSS) vulnerability. Successful exploit requires the attacker to know specific information about the target instance and trick a privileged user into clicking a specially crafted link. This could allow the attacker to view or modify configuration settings or add or modify user accounts.	2024-02-16	5.9	CVE-2024-21984
onnx -- onnx	Versions of the package onnx before and including 1.15.0 are vulnerable to Out-of-bounds Read as the ONNX_ASSERT and ONNX_ASSERTM functions have an off by one string copy.	2024-02-23	4.4	CVE-2024-27319
oracle_corporation -- bi_publisher_(formerly_xml_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 and 7.0.0.0.0. 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	2024-02-17	5.4	CVE-2024-20980

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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).			
oracle_corporation -- business_intelligence_enterprise_edition	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: BI Platform Security). 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 Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and 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 update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition 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).	2024-02-17	5.4	CVE-2024-20913
oracle_corporation -- common_applications	Vulnerability in the Oracle Common Applications product of Oracle E-Business Suite (component: CRM User Management Framework). 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 Common Applications. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Applications, 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 Common Applications accessible data as well as unauthorized read access to a subset of Oracle Common Applications 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).	2024-02-17	5.4	CVE-2024-20947
oracle_corporation -- crm_technical_foundation	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Admin Console). 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 CRM Technical Foundation. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle CRM Technical Foundation. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	2024-02-17	4.3	CVE-2024-20939
oracle_corporation -- 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 low privileged 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 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).	2024-02-17	5.4	CVE-2024-20958
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: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition executes 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	2024-02-17	4.7	CVE-2024-20945

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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 4.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N).			
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. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).	2024-02-17	5.9	CVE-2024-20919
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 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).	2024-02-17	5.9	CVE-2024-20921
oracle_corporation -- jd_edwards_enterpriseone_tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Monitoring and Diagnostics SEC). Supported versions that are affected are Prior to 9.2.8.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2024-02-17	4.3	CVE-2024-20937
oracle_corporation -- knowledge_management	Vulnerability in the Oracle Knowledge Management 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 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	2024-02-17	5.4	CVE-2024-20943

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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).			
oracle_corporation -- myqsl_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Difficult to exploit 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 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	2024-02-17	5.3	CVE-2024-20964
oracle_corporation -- mysql_server	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).	2024-02-17	4.9	CVE-2024-20966
oracle_corporation -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Difficult to exploit 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 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-02-17	4.4	CVE-2024-20968
oracle_corporation -- mysql_server	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).	2024-02-17	4.9	CVE-2024-20970
oracle_corporation -- mysql_server	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).	2024-02-17	4.9	CVE-2024-20972
oracle_corporation -- mysql_server	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).	2024-02-17	4.9	CVE-2024-20974
oracle_corporation -- mysql_server	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	2024-02-17	4.9	CVE-2024-20976

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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).			
oracle_corporation -- mysql_server	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).	2024-02-17	4.9	CVE-2024-20978
oracle_corporation -- mysql_server	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).	2024-02-17	4.9	CVE-2024-20982
oracle_corporation -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server : Security : Firewall). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Difficult to exploit 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 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-02-17	4.4	CVE-2024-20984
oracle_corporation -- sun_zfs_storage_appliance_kit_(ak)_software	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Object Store). The supported version that is affected is 8.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP 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 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2024-02-17	4.3	CVE-2023-21833
oracle_corporation -- application_object_library	Vulnerability in the Oracle Application Object Library product of Oracle E-Business Suite (component: Login - SSO). 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 Application Object Library. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Application Object Library. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2024-02-17	5.3	CVE-2024-20915
pinterest -- querybook	Querybook is a user interface for querying big data. Prior to version 3.31.1, there is a vulnerability in Querybook's rich text editor that enables users to input arbitrary URLs without undergoing necessary validation. This particular security flaw allows the use of `javascript:` protocol which can potentially trigger arbitrary client-side execution. The most extreme exploit of this flaw could occur when an admin user unknowingly clicks on a cross-site scripting URL, thereby unintentionally compromising admin role access to the attacker. A patch to rectify this issue has been introduced in Querybook version `3.31.1`. The fix is backward compatible and automatically fixes existing DataDocs. There are no known workarounds for this issue, except for manually checking each URL prior to clicking on them.	2024-02-21	6.1	CVE-2024-26148

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
presstigers -- simple_job_board	The Simple Job Board plugin for WordPress is vulnerable to unauthorized access of data| due to insufficient authorization checking on the fetch_quick_job() function in all versions up to, and including, 2.10.8. This makes it possible for unauthenticated attackers to fetch arbitrary posts, which can be password protected or private and contain sensitive information.	2024-02-21	5.3	CVE-2024-0593
prestashop -- prestashop	PrestaShop is an open-source e-commerce platform. Starting in version 8.1.0 and prior to version 8.1.4, PrestaShop is vulnerable to path disclosure in a JavaScript variable. A patch is available in version 8.1.4.	2024-02-19	5.8	CVE-2024-26129
raaj_trambadia -- pexels:_free_stock_photos	Server-Side Request Forgery (SSRF) vulnerability in Raaj Trambadia Pexels: Free Stock Photos.This issue affects Pexels: Free Stock Photos: from n/a through 1.2.2.	2024-02-23	4.9	CVE-2024-25915
redhat -- openshift	A flaw was found in OpenShift. The existing Cross-Site Request Forgery (CSRF) protections in place do not properly protect GET requests, allowing for the creation of WebSockets via CSRF.	2024-02-16	5.4	CVE-2024-1342
shopwind -- shopwind	A vulnerability was found in Shopwind up to 4.6. It has been rated as critical. This issue affects the function actionCreate of the file /public/install/controllers/DefaultController.php of the component Installation. The manipulation leads to code injection. 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 identifier VDB-254393 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-21	5.6	CVE-2024-1705
silabs.com -- ember_znet_sdk	Ember ZNet between v7.2.0 and v7.4.0 used software AES-CCM instead of integrated hardware cryptographic accelerators, potentially increasing risk of electromagnetic and differential power analysis sidechannel attacks.	2024-02-23	6.2	CVE-2023-51392
silabs.com -- ember_znet_sdk	Due to an allocation of resources without limits, an uncontrolled resource consumption vulnerability exists in Silicon Labs Ember ZNet SDK prior to v7.4.0.0 (delivered as part of Silicon Labs Gecko SDK v4.4.0) which may enable attackers to trigger a bus fault and crash of the device, requiring a reboot in order to rejoin the network.	2024-02-23	5.3	CVE-2023-51393
silabs.com -- ember_znet_sdk	High traffic environments may result in NULL Pointer Dereference vulnerability in Silicon Labs's Ember ZNet SDK before v7.4.0, causing a system crash.	2024-02-23	5.3	CVE-2023-51394
silabs.com -- gsdk	TRNG is used before initialization by ECDSA signing driver when exiting EM2/EM3 on Virtual Secure Vault (VSE) devices. This defect may allow Signature Spoofing by Key Recreation.This issue affects Gecko SDK through v4.4.0.	2024-02-21	6.8	CVE-2024-22473
silabs.com -- pc_controller	Malformed Device Reset Locally Command Class packets can be sent to the controller, causing the controller to assume the end device has left the network. After this, frames sent by the end device will not be acknowledged by the controller. This vulnerability exists in PC Controller v5.54.0, and earlier.	2024-02-21	6.5	CVE-2023-6533
silabs.com -- pc_controller	Malformed S2 Nonce Get Command Class packets can be sent to crash PC Controller v5.54.0 and earlier.	2024-02-21	6.5	CVE-2023-6640
silicon_labs -- gecko_platform	A denial of service vulnerability exists in the ICMP and ICMPv6 parsing functionality of Weston Embedded uC-TCP-IP v3.06.01. A specially crafted network packet can lead to an out-of-bounds read. An attacker can send a malicious packet to trigger this vulnerability.This vulnerability concerns a denial of service within the parsing an IPv4 ICMP packet.	2024-02-20	5.9	CVE-2023-39540
silicon_labs -- gecko_platform	A denial of service vulnerability exists in the ICMP and ICMPv6 parsing functionality of Weston Embedded uC-TCP-IP v3.06.01. A specially crafted network packet can lead to an out-of-bounds read. An attacker can send a malicious packet to trigger	2024-02-20	5.9	CVE-2023-39541

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	this vulnerability.This vulnerability concerns a denial of service within the parsing an IPv6 ICMPv6 packet.			
smub -- user_feedback_create_interactive_feedback_form,_user_surveys,_and_polls_in_seconds	The User Feedback - Create Interactive Feedback Form, User Surveys, and Polls in Seconds plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'page_submitted' 'link' value in all versions up to, and including, 1.0.13 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in the feedback submission page that will execute when a user clicks the link, while also pressing the command key.	2024-02-22	5.4	CVE-2024-0903
softaculous -- page_builder:_pagelayer_drag_and_drop_website_builder	The Page Builder: Pagelayer - Drag and Drop website builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Button Widget in all versions up to, and including, 1.8.2 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.	2024-02-23	4.6	CVE-2024-1590
sonicwall -- sma100	Improper access control vulnerability has been identified in the SMA100 SSL-VPN virtual office portal, which in specific conditions could potentially enable a remote authenticated attacker to associate another user's MFA mobile application.	2024-02-24	6.3	CVE-2024-22395 PSIRT@sonicwall.com
soninow_team -- dugbug	Cross-Site Request Forgery (CSRF) vulnerability in SoniNow Team Debug.This issue affects Debug: from n/a through 1.10.	2024-02-21	4.3	CVE-2024-24798
temmoki_mvc -- tommoku_mvc	A vulnerability, which was classified as critical, was found in TemmokuMVC up to 2.3. Affected is the function get_img_url/img_replace in the library lib/images_get_down.php of the component Image Download Handler. 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-254532. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-22	5.6	CVE-2024-1750
theeventscalendar -- event_tickets_and_registration	The Event Tickets and Registration plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'email' action in all versions up to, and including, 5.8.1. This makes it possible for authenticated attackers, with contributor-level access and above, to email the attendees list to themselves.	2024-02-22	4.3	CVE-2024-1053
themify -- themify_builder	Cross-Site Request Forgery (CSRF) vulnerability in Themify Themify Builder.This issue affects Themify Builder: from n/a through 7.0.5.	2024-02-21	4.3	CVE-2024-24872
totolink -- x6000r_ax3000	A vulnerability was found in Totolink X6000R AX3000 9.4.0cu.852_20230719. It has been rated as critical. This issue affects the function setWizardCfg of the file /cgi-bin/cstecgi.cgi of the component shttpd. The manipulation leads to command injection. The exploit has been disclosed to the public and may be used. The identifier VDB-254573 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-23	6.3	CVE-2024-1781
van_der_schaar_lab -- autoprognosis	A vulnerability classified as critical was found in van_der_Schaar LAB AutoPrognosis 0.1.21. This vulnerability affects the function load_model_from_file of the component Release Note Handler. The manipulation leads to deserialization. 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-254530 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-22	5	CVE-2024-1748

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
videolan -- dav1d	An integer overflow in dav1d AV1 decoder that can occur when decoding videos with large frame size. This can lead to memory corruption within the AV1 decoder. We recommend upgrading past version 1.4.0 of dav1d.	2024-02-19	5.9	CVE-2024-1580
vmware -- aria_operations	VMware Aria Operations contains a local privilege escalation vulnerability. A malicious actor with administrative access to the local system can escalate privileges to 'root'.	2024-02-21	6.7	CVE-2024-22235
webfactory -- databasereset	The Database Reset plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.22. This is due to missing or incorrect nonce validation on the install_wpr() function. This makes it possible for unauthenticated attackers to install the WP Reset Plugin via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-02-21	4.7	CVE-2024-1501
westerndeal -- woocommerce_google_sheet_connector	The WooCommerce Google Sheet Connector plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the execute_post_data function in all versions up to, and including, 1.3.11. This makes it possible for unauthenticated attackers to update plugin settings.	2024-02-21	5.3	CVE-2024-1562
wolfssl -- wolfssl	In wolfSSL prior to 5.6.6, if callback functions are enabled (via the WOLFSSL_CALLBACKS flag), then a malicious TLS client or network attacker can trigger a buffer over-read on the heap of 5 bytes (WOLFSSL_CALLBACKS is only intended for debugging).	2024-02-20	5.3	CVE-2023-6936
xwikisas -- application-licensing	The XWiki licensor application, which manages and enforce application licenses for paid extensions, includes the document `Licenses.Code.LicenseJSON` that provides information for admins regarding active licenses. This document is public and thus exposes this information publicly. The information includes the instance's id as well as first and last name and email of the license owner. This is a leak of information that isn't supposed to be public. The instance id allows associating data on the active installs data with the concrete XWiki instance. Active installs assures that "there's no way to find who's having a given UUID" (referring to the instance id). Further, the information who the license owner is and information about the obtained licenses can be used for targeted phishing attacks. Also, while user information is normally public, email addresses might only be displayed obfuscated, depending on the configuration. This has been fixed in Application Licensing 1.24.2. There are no known workarounds besides upgrading.	2024-02-21	5.3	CVE-2024-26138
yetanalytics -- lrs	com.yetanalytics/lrs is the Yet Analytics Core LRS Library. Prior to version 1.2.17 of the LRS library and version 0.7.5 of SQL LRS, a maliciously crafted xAPI statement could be used to perform script or other tag injection in the LRS Statement Browser. The problem is patched in version 1.2.17 of the LRS library and version 0.7.5 of SQL LRS. No known workarounds exist.	2024-02-20	4.6	CVE-2024-26140
zephyrproject-rtos -- zephyr	can: out of bounds in remove_rx_filter function	2024-02-18	4.4	CVE-2023-5779
zestardtechnologies -- admin_side_data_storage_for_contact_form_7	The Admin side data storage for Contact Form 7 plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.1. This is due to missing or incorrect nonce validation on the settings update function. This makes it possible for unauthenticated attackers to update 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.	2024-02-23	4.3	CVE-2024-1777
zestardtechnologies -- admin_side_data_storage_for_contact_form_7	The Admin side data storage for Contact Form 7 plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the zt_dcfcf_change_bookmark() function in all versions up to, and including, 1.1.1. This makes it possible for unauthenticated attackers to alter bookmark statuses.	2024-02-23	4.3	CVE-2024-1778

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zestardtechnologies -- admin_side_data_storage_for_contact_form_7	The Admin side data storage for Contact Form 7 plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the zt_dcfcf_change_status() function in all versions up to, and including, 1.1.1. This makes it possible for unauthenticated attackers to alter the message read status of messages.	2024-02-23	5.3	CVE-2024-1779
zhongbangkeji -- crmeb	A vulnerability was found in ZhongBangKeJi CRMEB 5.2.2. It has been declared as critical. This vulnerability affects the function save/delete of the file /adminapi/system/crud. The manipulation leads to path traversal. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-254392. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-21	5.5	CVE-2024-1704
zyxel -- atp_series_firmware	A null pointer dereference vulnerability in Zyxel ATP series firmware versions from 4.32 through 5.37 Patch 1 and USG FLEX series firmware versions from 4.50 through 5.37 Patch 1 could allow a LAN-based attacker to cause denial-of-service (DoS) conditions by downloading a crafted RAR compressed file onto a LAN-side host if the firewall has the "Anti-Malware" feature enabled.	2024-02-20	6.5	CVE-2023-6397
zyxel -- atp_series_firmware	A format string vulnerability in Zyxel ATP series firmware versions from 4.32 through 5.37 Patch 1, USG FLEX series firmware versions from 4.50 through 5.37 Patch 1, USG FLEX 50(W) series firmware versions from 4.16 through 5.37 Patch 1, USG20(W)-VPN series firmware versions from 4.16 through 5.37 Patch 1, and USG FLEX H series firmware versions from 1.10 through 1.10 Patch 1 could allow an authenticated IPSec VPN user to cause DoS conditions against the "deviceid" daemon by sending a crafted hostname to an affected device if it has the "Device Insight" feature enabled.	2024-02-20	5.7	CVE-2023-6399
adobe -- acrobat_reader	Acrobat Reader versions 20.005.30539, 23.008.20470 and earlier are affected by an Improper Input Validation vulnerability that could lead to an application denial-of-service. An attacker could leverage this vulnerability to cause the application to crash, resulting in a denial of service. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	5.5	CVE-2024-20733
adobe -- acrobat_reader	Acrobat Reader versions 20.005.30539, 23.008.20470 and earlier are affected by a Use After Free 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.	2024-02-15	5.5	CVE-2024-20734
adobe -- acrobat_reader	Acrobat Reader versions 20.005.30539, 23.008.20470 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.	2024-02-15	5.5	CVE-2024-20735
adobe -- acrobat_reader	Acrobat Reader versions 20.005.30539, 23.008.20470 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.	2024-02-15	5.5	CVE-2024-20736
adobe -- acrobat_reader	Acrobat Reader versions 20.005.30539, 23.008.20470 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.	2024-02-15	5.5	CVE-2024-20747
adobe -- acrobat_reader	Acrobat Reader versions 20.005.30539, 23.008.20470 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	2024-02-15	5.5	CVE-2024-20748

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
adobe -- acrobat_reader	Acrobat Reader versions 20.005.30539, 23.008.20470 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.	2024-02-15	5.5	CVE-2024-20749
adobe -- commerce	Adobe Commerce versions 2.4.6-p3, 2.4.5-p5, 2.4.4-p6 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to trick a victim into performing actions they did not intend to do, which could be used to bypass security measures and gain unauthorized access. Exploitation of this issue requires user interaction, typically in the form of the victim clicking a link or visiting a malicious website.	2024-02-15	6.5	CVE-2024-20718
adobe -- commerce	Adobe Commerce versions 2.4.6-p3, 2.4.5-p5, 2.4.4-p6 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.	2024-02-15	5.4	CVE-2024-20717
adobe -- commerce	Adobe Commerce versions 2.4.6-p3, 2.4.5-p5, 2.4.4-p6 and earlier are affected by an Uncontrolled Resource Consumption vulnerability that could lead to an application denial-of-service. A high-privileged attacker could leverage this vulnerability to exhaust system resources, causing the application to slow down or crash. Exploitation of this issue does not require user interaction.	2024-02-15	4.9	CVE-2024-20716
adobe -- substance_3d_painter	Substance3D - Painter versions 9.1.1 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.	2024-02-15	5.5	CVE-2024-20722
adobe -- substance_3d_painter	Substance3D - Painter versions 9.1.1 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.	2024-02-15	5.5	CVE-2024-20724
adobe -- substance_3d_painter	Substance3D - Painter versions 9.1.1 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.	2024-02-15	5.5	CVE-2024-20725
algosec -- algosec_fireflow	Improper input validation in Algosec FireFlow VisualFlow workflow editor via Name, Description and Configuration File field in version A32.20, A32.50, A32.60 permits an attacker to initiate an XSS attack by injecting malicious executable scripts into the application's code. Fixed in version A32.20 (b600 and above), A32.50 (b430 and above), A32.60 (b250 and above)	2024-02-15	5.1	CVE-2023-46596
apache_software_foundation -- apache_superset	This is a duplicate for CVE-2023-46104. With correct CVE version ranges for affected Apache Superset. Uncontrolled resource consumption can be triggered by authenticated attacker that uploads a malicious ZIP to import database, dashboards or datasets. This vulnerability exists in Apache Superset versions up to and including 2.1.2 and versions 3.0.0, 3.0.1.	2024-02-14	6.5	CVE-2024-23952
ari_soft -- contact_form_7_connector	Cross-Site Request Forgery (CSRF) vulnerability in ARI Soft Contact Form 7 Connector. This issue affects Contact Form 7 Connector: from n/a through 1.2.2.	2024-02-12	4.3	CVE-2024-24884

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
automattic -- crowdsignal_dashboard	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Automattic, Inc. Crowdsignal Dashboard - Polls, Surveys & more allows Reflected XSS. This issue affects Crowdsignal Dashboard - Polls, Surveys & more: from n/a through 3.0.11.	2024-02-10	6.1	CVE-2023-51488
automattic -- sensei_lms	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Automatic Sensei LMS - Online Courses, Quizzes, & Learning allows Stored XSS. This issue affects Sensei LMS - Online Courses, Quizzes, & Learning: from n/a through 4.17.0.	2024-02-12	5.4	CVE-2023-50875
axiosys -- bento4	Bento4 v1.6.0-640 was discovered to contain an out-of-memory bug via the AP4_DataBuffer::ReallocateBuffer() function.	2024-02-09	6.5	CVE-2024-25451
axiosys -- bento4	Bento4 v1.6.0-640 was discovered to contain an out-of-memory bug via the AP4_UrlAtom::AP4_UrlAtom() function.	2024-02-09	5.5	CVE-2024-25452
axiosys -- bento4	Bento4 v1.6.0-640 was discovered to contain a NULL pointer dereference via the AP4_StszAtom::GetSampleSize() function.	2024-02-09	5.5	CVE-2024-25453
axiosys -- bento4	Bento4 v1.6.0-640 was discovered to contain a NULL pointer dereference via the AP4_DescriptorFinder::Test() function.	2024-02-09	5.5	CVE-2024-25454
ays-pro -- chartify	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Chart Builder Team Chartify - WordPress Chart Plugin allows Stored XSS.This issue affects Chartify - WordPress Chart Plugin: from n/a through 2.0.6.	2024-02-12	4.8	CVE-2023-47526
badge -- hacker_hotel_badge	Allocation of Resources Without Limits or Throttling vulnerability in Badge leading to a denial-of-service attack. Team Hacker Hotel Badge 2024 on risc-v (billboard modules) allows Flooding. This issue affects Hacker Hotel Badge 2024: from 0.1.0 through 0.1.3.	2024-02-11	5.7	CVE-2024-21875
barangay_management_system_project -- barangay_management_system	Barangay Population Monitoring System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the Add Resident function at /barangay-population-monitoring-system/masterlist.php. This vulnerabiity allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Contact Number parameter.	2024-02-14	5.4	CVE-2024-25207
barangay_management_system_project -- barangay_management_system	Barangay Population Monitoring System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the Add Resident function at /barangay-population-monitoring-system/masterlist.php. This vulnerabiity allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Full Name parameter.	2024-02-14	5.4	CVE-2024-25208
beds24 -- online_booking	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mark Kinchin Beds24 Online Booking allows Stored XSS.This issue affects Beds24 Online Booking: from n/a through 2.0.23.	2024-02-10	4.8	CVE-2024-24717
beyondtrust -- privilege_management_for_windows	An issue was discovered in BeyondTrust Privilege Management for Windows before 24.1. When a low-privileged user initiates a repair, there is an attack vector through which the user is able to execute any program with elevated privileges.	2024-02-16	6.3	CVE-2024-25083
calculatorsworld -- cc_bmi_calculator	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Calculators World CC BMI Calculator allows Stored XSS.This issue affects CC BMI Calculator: from n/a through 2.0.1.	2024-02-10	5.4	CVE-2024-23516
canonical_ltd -- lxd	An insecure default to allow UEFI Shell in EDK2 was left enabled in Ubuntu's EDK2. This allows an OS-resident attacker to bypass Secure Boot.	2024-02-14	6.7	CVE-2023-48733

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
canonical_ltd -- lxd	An insecure default to allow UEFI Shell in EDK2 was left enabled in LXD. This allows an OS-resident attacker to bypass Secure Boot.	2024-02-14	6.7	CVE-2023-49721
clicktotweet -- click_to_tweet	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ClickToTweet.Com Click To Tweet allows Stored XSS.This issue affects Click To Tweet: from n/a through 2.0.14.	2024-02-10	5.4	CVE-2024-23514
comarch -- erp_xl	The database access credentials configured during installation are stored in a special table, and are encrypted with a shared key, same among all Comarch ERP XL client installations. This could allow an attacker with access to that table to retrieve plain text passwords. This issue affects ERP XL: from 2020.2.2 through 2023.2.	2024-02-15	6.2	CVE-2023-4538
concretecms -- concrete_cms	Concrete CMS version 9 before 9.2.5 is vulnerable to stored XSS in file tags and description attributes since administrator entered file attributes are not sufficiently sanitized in the Edit Attributes page. A rogue administrator could put malicious code into the file tags or description attributes and, when another administrator opens the same file for editing, the malicious code could execute. The Concrete CMS Security team scored this 2.4 with CVSS v3 vector AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N.	2024-02-09	4.8	CVE-2024-1245
concretecms -- concrete_cms	Concrete CMS in version 9 before 9.2.5 is vulnerable to reflected XSS via the Image URL Import Feature due to insufficient validation of administrator provided data. A rogue administrator could inject malicious code when importing images, leading to the execution of the malicious code on the website user's browser. The Concrete CMS Security team scored this 2 with CVSS v3 vector AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N. This does not affect Concrete versions prior to version 9.	2024-02-09	4.8	CVE-2024-1246
concretecms -- concrete_cms	Concrete CMS version 9 before 9.2.5 is vulnerable to stored XSS via the Role Name field since there is insufficient validation of administrator provided data for that field. A rogue administrator could inject malicious code into the Role Name field which might be executed when users visit the affected page. The Concrete CMS Security team scored this 2 with CVSS v3 vector AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator . Concrete versions below 9 do not include group types so they are not affected by this vulnerability.	2024-02-09	4.8	CVE-2024-1247
content_cards_project -- content_cards	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Arunas Liuiza Content Cards allows Stored XSS.This issue affects Content Cards: from n/a through 0.9.7.	2024-02-12	5.4	CVE-2024-24928
dell -- bsafe_ssl-j	Dell BSAFE SSL-J, versions prior to 6.5, and versions 7.0 and 7.1 contain a debug message revealing unnecessary information vulnerability. This may lead to disclosing sensitive information to a locally privileged user.	2024-02-10	4.4	CVE-2023-28077
dell -- mobility_e-lab_navigator	Dell E-Lab Navigator, [3.1.9, 3.2.0], contains an Insecure Direct Object Reference Vulnerability in Feedback submission. An attacker could potentially exploit this vulnerability, to manipulate the email's appearance, potentially deceiving recipients and causing reputational and security risks.	2024-02-14	4.4	CVE-2024-22455
dell -- recoverpoint_for_vms	Dell RecoverPoint for Virtual Machines 5.3.x contains a brute force/dictionary attack vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to launch a brute force attack or a dictionary attack against the RecoverPoint login form. This allows attackers to brute-force the password of valid users in an automated manner.	2024-02-16	6.5	CVE-2024-22425
dell -- secure_connect_g	In Dell Secure Connect Gateway Application and Secure Connect Gateway Appliance (between v5.10.00.00 and v5.18.00.00), a security concern has been identified, where a malicious user with a valid User session may inject malicious	2024-02-14	5.4	CVE-2023-44293

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ateway-application	content in filters of IP Range Rest API. This issue may potentially lead to unintentional information disclosure from the product database.			
dell -- secure_connect_gateway-application	In Dell Secure Connect Gateway Application and Secure Connect Gateway Appliance (between v5.10.00.00 and v5.18.00.00), a security concern has been identified, where a malicious user with a valid User session may inject malicious content in filters of Collection Rest API. This issue may potentially lead to unintentional information disclosure from the product database.	2024-02-14	5.4	CVE-2023-44294
dell -- supportassist_client_consumer	Dell SupportAssist for Business PCs version 3.4.0 contains a local Authentication Bypass vulnerability that allows locally authenticated non-admin users to gain temporary privilege within the SupportAssist User Interface on their respective PC. The Run as Admin temporary privilege feature enables IT/System Administrators to perform driver scans and Dell-recommended driver installations without requiring them to log out of the local non-admin user session. However, the granted privilege is limited solely to the SupportAssist User Interface and automatically expires after 15 minutes.	2024-02-14	6.3	CVE-2023-39249
dell -- unity_operating_environment	Dell Unity, versions prior to 5.4, contains SQL Injection vulnerability. An authenticated attacker could potentially exploit this vulnerability, leading to exposure of sensitive information.	2024-02-12	6.5	CVE-2024-22221
dell -- unity_operating_environment	Dell Unity, versions prior to 5.4, contain a path traversal vulnerability in its svc_supportassist utility. An authenticated attacker could potentially exploit this vulnerability, to gain unauthorized write access to the files stored on the server filesystem, with elevated privileges.	2024-02-12	6.5	CVE-2024-22226
dell -- unity_operating_environment	Dell Unity, versions prior to 5.4, contains a cross-site scripting (XSS) vulnerability. An authenticated attacker could potentially exploit this vulnerability, leading users to download and execute malicious software crafted by this product's feature to compromise their systems.	2024-02-12	5.4	CVE-2024-0169
dell -- unity_operating_environment	Dell Unity, versions prior to 5.4, contains a Cross-site scripting vulnerability. An authenticated attacker could potentially exploit this vulnerability, stealing session information, masquerading as the affected user or carry out any actions that this user could perform, or to generally control the victim's browser.	2024-02-12	5.4	CVE-2024-22230
derhansen -- sf_event_mgt	sf_event_mgt is an event management and registration extension for the TYPO3 CMS based on ExtBase and Fluid. In affected versions the existing access control check for events in the backend module got broken during the update of the extension to TYPO3 12.4, because the `RedirectResponse` from the `$this->redirect()` function was never handled. This issue has been addressed in version 7.4.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-13	4.3	CVE-2024-24751
ebm_technologies -- risweb	EBM Technologies RISWEB's specific URL path is not properly controlled by permission, allowing attackers to browse specific pages and query sensitive data without login.	2024-02-15	5.3	CVE-2024-26263
ecshop -- ecshop	A vulnerability, which was classified as critical, has been found in ECshop 4.1.8. Affected by this issue is some unknown functionality of the file /admin/view_sendlist.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-250562 is the identifier assigned to this vulnerability.	2024-02-15	6.3	CVE-2024-1530
envoyproxy -- envoy	Envoy is a high-performance edge/middle/service proxy. The regex expression is compiled for every request and can result in high CPU usage and increased request latency when multiple routes are configured with such matchers. This issue has been addressed in released 1.29.1, 1.28.1, 1.27.3, and 1.26.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-09	5.3	CVE-2024-23323

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
exiv2 -- exiv2	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An out-of-bounds read was found in Exiv2 version v0.28.1. The vulnerable function, `QuickTimeVideo::NikonTagsDecoder`, was new in v0.28.0, so Exiv2 versions before v0.28 are _not_ affected. The out-of-bounds read is triggered when Exiv2 is used to read the metadata of a crafted video file. In most cases this out of bounds read will result in a crash. This bug is fixed in version v0.28.2. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-12	5.5	CVE-2024-24826
exiv2 -- exiv2	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. A denial-of-service was found in Exiv2 version v0.28.1: an unbounded recursion can cause Exiv2 to crash by exhausting the stack. The vulnerable function, `QuickTimeVideo::multipleEntriesDecoder`, was new in v0.28.0, so Exiv2 versions before v0.28 are _not_ affected. The denial-of-service is triggered when Exiv2 is used to read the metadata of a crafted video file. This bug is fixed in version v0.28.2. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-12	5.5	CVE-2024-25112
f5 -- big-ip	BIG-IP or BIG-IQ Resource Administrators and Certificate Managers who have access to the secure copy (scp) utility but do not have access to Advanced shell (bash) can execute arbitrary commands with a specially crafted command string. This vulnerability is due to an incomplete fix for CVE-2020-5873. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2024-02-14	6.7	CVE-2024-21782
f5 -- big-ip	When running in Appliance mode, an authenticated attacker assigned the Administrator role may be able to bypass Appliance mode restrictions utilizing iAppsLX templates on a BIG-IP system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2024-02-14	6	CVE-2024-23976
f5 -- big-ip_next_spk	A vulnerability exists in BIG-IP Next CNF and SPK systems that may allow access to undisclosed sensitive files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2024-02-14	4.4	CVE-2024-23306
f5 -- f5os_-_appliance	When LDAP remote authentication is configured on F5OS, a remote user without an assigned role will be incorrectly authorized. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-02-14	6.2	CVE-2024-24966
f5 -- f5os_-_appliance	A directory traversal vulnerability exists in the F5OS QKView utility that allows an authenticated attacker to read files outside the QKView directory. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-02-14	5.5	CVE-2024-23607
filseclab -- twister_antivirus	Twister Antivirus v8.17 is vulnerable to an Out-of-bounds Read vulnerability by triggering the 0x801120B8 IOCTL code of the filmfd.sys driver.	2024-02-13	5.8	CVE-2024-1140
filseclab -- twister_antivirus	Twister Antivirus v8.17 is vulnerable to a Denial-of-Service vulnerability by triggering the 0x80112044, 0x8011204B, 0x8011204F, 0x80112057, 0x8011205B, 0x8011205F, 0x80112063, 0x8011206F, 0x80112073, 0x80112077, 0x80112078, 0x8011207C and 0x80112080 IOCTL codes of the fildds.sys driver.	2024-02-13	5.5	CVE-2024-1216
fortinet -- fortimanager	An exposure of sensitive information to an unauthorized actor vulnerability [CWE-200] in Fortinet FortiManager version 7.4.0 through 7.4.1 and before 7.2.5, FortiAnalyzer version 7.4.0 through 7.4.1 and before 7.2.5 and FortiAnalyzer-BigData before 7.2.5 allows an adom administrator to enumerate other adoms and device names via crafted HTTP or HTTPS requests.	2024-02-15	5	CVE-2023-44253
fortinet -- fortinac	An improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiNAC 9.4.0 - 9.4.2, 9.2.0 - 9.2.8, 9.1.0 - 9.1.10 and 7.2.0 allows an attacker to execute unauthorized code or commands via the name fields observed in the policy audit logs.	2024-02-15	6.8	CVE-2023-26206

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fortinet -- fortios	An improper certificate validation vulnerability in Fortinet FortiOS 7.0.0 - 7.0.13, 7.2.0 - 7.2.6 and 7.4.0 - 7.4.1 allows a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the FortiLink communication channel between the FortiOS device and FortiSwitch.	2024-02-15	4.8	CVE-2023-47537
geek_code_lab -- all_404_pages_redirect_to_homepage	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Geek Code Lab All 404 Pages Redirect to Homepage allows Stored XSS. This issue affects All 404 Pages Redirect to Homepage: from n/a through 1.9.	2024-02-12	6.1	CVE-2024-24889
getawesomesupport -- awesome_support	The Awesome Support - WordPress HelpDesk & Support Plugin plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the wpas_get_users() function hooked via AJAX in all versions up to, and including, 6.1.7. This makes it possible for authenticated attackers, with subscriber-level access and above, to retrieve user data such as emails.	2024-02-10	4.3	CVE-2024-0595
getgrav -- grav	A cross-site scripting (XSS) vulnerability in Grav versions 1.7.44 and before, allows remote authenticated attackers to execute arbitrary web scripts or HTML via the onmouseover attribute of an ISINDEX element.	2024-02-09	5.4	CVE-2023-31506
github -- enterprise_server	A path traversal vulnerability was identified in GitHub Enterprise Server that allowed an attacker to gain unauthorized read permission to files by deploying arbitrary symbolic links to a GitHub Pages site with a specially crafted artifact tarball. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.8.15, 3.9.10, 3.10.7, 3.11.5. This vulnerability was reported via the GitHub Bug Bounty program.	2024-02-13	6.3	CVE-2024-1082
github -- enterprise_server	Cross-site Scripting in the tag name pattern field in the tag protections UI in GitHub Enterprise Server allows a malicious website that requires user interaction and social engineering to make changes to a user account via CSP bypass with created CSRF tokens. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in all versions of 3.11.5, 3.10.7, 3.9.10, and 3.8.15. This vulnerability was reported via the GitHub Bug Bounty program.	2024-02-13	6.5	CVE-2024-1084
gitlab -- gitlab	An issue has been discovered in GitLab EE affecting all versions starting from 16.8 before 16.8.2. When a user is assigned a custom role with manage_group_access_tokens permission, they may be able to create group access tokens with Owner privileges, which may lead to privilege escalation.	2024-02-12	6.5	CVE-2024-1250
givewp -- givewp	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GiveWP GiveWP - Donation Plugin and Fundraising Platform allows Stored XSS. This issue affects GiveWP - Donation Plugin and Fundraising Platform: from n/a through 3.2.2.	2024-02-10	5.4	CVE-2023-51415
glewlwyd_sso_server_project -- glewlwyd_sso_server	Glewlwyd SSO server 2.x through 2.7.6 allows open redirection via redirect_uri.	2024-02-11	6.1	CVE-2024-25715
grafana -- grafana	A user changing their email after signing up and verifying it can change it without verification in profile settings. The configuration option "verify_email_enabled" will only validate email only on sign up.	2024-02-13	5.4	CVE-2023-6152
grafana -- grafana-csv-datasource	Grafana is an open-source platform for monitoring and observability. The CSV datasource plugin is a Grafana Labs maintained plugin for Grafana that allows for retrieving and processing CSV data from a remote endpoint configured by an administrator. If this plugin was configured to send requests to a bare host with no path (e.g. https://www.example.com/ https://www.example.com/`), requests to an endpoint other than the one configured by the administrator could be triggered	2024-02-14	5	CVE-2023-5122

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	by a specially crafted request from any user, resulting in an SSRF vector. AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator			
greenpau -- github.com/greenpau/caddy-security	Versions of the package github.com/greenpau/caddy-security before 1.0.42 are vulnerable to Insecure Randomness due to using an insecure random number generation library which could possibly be predicted via a brute-force search. Attackers could use the potentially predictable nonce value used for authentication purposes in the OAuth flow to conduct OAuth replay attacks. In addition, insecure randomness is used while generating multifactor authentication (MFA) secrets and creating API keys in the database package.	2024-02-17	6.5	CVE-2024-21495
greenpau -- github.com/greenpau/caddy-security	All versions of the package github.com/greenpau/caddy-security are vulnerable to Cross-site Scripting (XSS) via the Referer header, due to improper input sanitization. Although the Referer header is sanitized by escaping some characters that can allow XSS (e.g., [&], [<], [>], ["], ['']), it does not account for the attack based on the JavaScript URL scheme (e.g., javascript:alert(document.domain)// payload). Exploiting this vulnerability may not be trivial, but it could lead to the execution of malicious scripts in the context of the target user's browser, compromising user sessions.	2024-02-17	6.1	CVE-2024-21496
greenpau -- github.com/greenpau/caddy-security	All versions of the package github.com/greenpau/caddy-security are vulnerable to Improper Validation of Array Index when parsing a Caddyfile. Multiple parsing functions in the affected library do not validate whether their input values are nil before attempting to access elements, which can lead to a panic (index out of range). Panics during the parsing of a configuration file may introduce ambiguity and vulnerabilities, hindering the correct interpretation and configuration of the web server.	2024-02-17	5.3	CVE-2024-21493
greenpau -- github.com/greenpau/caddy-security	All versions of the package github.com/greenpau/caddy-security are vulnerable to Authentication Bypass by Spoofing via the X-Forwarded-For header due to improper input sanitization. An attacker can spoof an IP address used in the user identity module (/whoami API endpoint). This could lead to unauthorized access if the system trusts this spoofed IP address.	2024-02-17	5.4	CVE-2024-21494
greenpau -- github.com/greenpau/caddy-security	All versions of the package github.com/greenpau/caddy-security are vulnerable to Open Redirect via the redirect_url parameter. An attacker could perform a phishing attack and trick users into visiting a malicious website by crafting a convincing URL with this parameter. To exploit this vulnerability, the user must take an action, such as clicking on a portal button or using the browser's back button, to trigger the redirection.	2024-02-17	5.4	CVE-2024-21497
greenpau -- github.com/greenpau/caddy-security	All versions of the package github.com/greenpau/caddy-security are vulnerable to Server-side Request Forgery (SSRF) via X-Forwarded-Host header manipulation. An attacker can expose sensitive information, interact with internal services, or exploit other vulnerabilities within the network by exploiting this vulnerability.	2024-02-17	5.3	CVE-2024-21498
greenpau -- github.com/greenpau/caddy-security	All versions of the package github.com/greenpau/caddy-security are vulnerable to Insufficient Session Expiration due to improper user session invalidation upon clicking the "Sign Out" button. User sessions remain valid even after requests are sent to /logout and /oauth2/google/logout. Attackers who gain access to an active, but supposedly logged-out session can perform unauthorized actions on behalf of the user.	2024-02-17	4.8	CVE-2024-21492
greenpau -- github.com/greenpau/caddy-security	All versions of the package github.com/greenpau/caddy-security are vulnerable to HTTP Header Injection via the X-Forwarded-Proto header due to redirecting to the injected protocol. Exploiting this vulnerability could lead to bypass of security mechanisms or confusion in handling TLS.	2024-02-17	4.3	CVE-2024-21499
greenpau -- github.com/greenp	All versions of the package github.com/greenpau/caddy-security are vulnerable to Improper Restriction of Excessive Authentication Attempts via the two-factor authentication (2FA). Although the application blocks the user after several failed	2024-02-17	4.8	CVE-2024-21500

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
au/caddy-security	attempts to provide 2FA codes, attackers can bypass this blocking mechanism by automating the application's full multistep 2FA process.			
hcl_software -- hcl_connections	HCL Connections is vulnerable to a denial of service, caused by improper validation on certain requests. Using a specially crafted request an attacker could exploit this vulnerability to cause denial of service for affected users.	2024-02-12	5.5	CVE-2023-28018
helm -- helm	Helm is a tool for managing Charts. Charts are packages of pre-configured Kubernetes resources. When either the Helm client or SDK is used to save a chart whose name within the `Chart.yaml` file includes a relative path change, the chart would be saved outside its expected directory based on the changes in the relative path. The validation and linting did not detect the path changes in the name. This issue has been resolved in Helm v3.14.1. Users unable to upgrade should check all charts used by Helm for path changes in their name as found in the `Chart.yaml` file. This includes dependencies.	2024-02-15	6.4	CVE-2024-25620
hima -- f30_03x_yy_(com)	An unauthenticated attacker can send a ping request from one network to another through an error in the origin verification even though the ports are separated by VLAN.	2024-02-13	4.3	CVE-2024-24782
howardehrenberg -- custom_post_carousels_with_owl	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Howard Ehrenberg Custom Post Carousels with Owl allows Stored XSS.This issue affects Custom Post Carousels with Owl: from n/a through 1.4.6.	2024-02-10	5.4	CVE-2023-51493
ibm -- cics_tx_standard	IBM CICS TX Standard and Advanced 11.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 229440.	2024-02-12	5.9	CVE-2022-34309
ibm -- cics_tx_standard	IBM CICS TX Standard and Advanced 11.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 229441.	2024-02-12	5.9	CVE-2022-34310
ibm -- cics_tx_standard	IBM CICS TX Standard and Advanced 11.1 could allow a user with physical access to the web browser to gain access to the user's session due to insufficiently protected credentials. IBM X-Force ID: 229446.	2024-02-12	4.3	CVE-2022-34311
ibm -- datastage_on_cloud_pak_for_data	IBM DataStage on Cloud Pak for Data 4.0.6 to 4.5.2 stores sensitive credential information that can be read by a privileged user. IBM X-Force ID: 235060.	2024-02-12	4.9	CVE-2022-38714
ibm -- engineering_lifecycle_optimization	IBM Engineering Lifecycle Optimization 7.0.2 and 7.0.3 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: 268754.	2024-02-09	6.1	CVE-2023-45190
ibm -- i_access_client_solutions	IBM i Access Client Solutions (ACS) 1.1.2 through 1.1.4 and 1.1.4.3 through 1.1.9.4 is vulnerable to NT LAN Manager (NTLM) hash disclosure by an attacker modifying UNC capable paths within ACS configuration files to point to a hostile server. If NTLM is enabled, the Windows operating system will try to authenticate using the current user's session. The hostile server could capture the NTLM hash information to obtain the user's credentials. IBM X-Force ID: 279091.	2024-02-09	5.5	CVE-2024-22318
ibm -- integration_bus	The IBM Integration Bus for z/OS 10.1 through 10.1.0.2 AdminAPI is vulnerable to a denial of service due to file system exhaustion. IBM X-Force ID: 279972.	2024-02-09	6.5	CVE-2024-22332
ibm -- jazz_for_service_management	IBM Jazz for Service Management 1.1.3.20 could allow an unauthorized user to obtain sensitive file information using forced browsing due to improper access controls. IBM X-Force ID: 269929.	2024-02-14	5.3	CVE-2023-46186

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- qradar_suite_software	IBM QRadar Suite 1.10.12.0 through 1.10.17.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 279975.	2024-02-17	5.1	CVE-2024-22335
ibm -- qradar_suite_software	IBM QRadar Suite 1.10.12.0 through 1.10.17.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 279976.	2024-02-17	5.1	CVE-2024-22336
ibm -- qradar_suite_software	IBM QRadar Suite 1.10.12.0 through 1.10.17.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 279977.	2024-02-17	5.1	CVE-2024-22337
ibm -- qradar_suite_software	IBM QRadar Suite 1.10.12.0 through 1.10.17.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 in some circumstances will log some sensitive information about invalid authorization attempts. IBM X-Force ID: 275747.	2024-02-17	4	CVE-2023-50951
ibm -- robotic_process_automation	IBM Robotic Process Automation 21.0.2 contains a vulnerability that could allow user ids may be exposed across tenants. IBM X-Force ID: 227293.	2024-02-12	4.6	CVE-2022-22506
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator 6.0.0.0 through 6.0.3.8 and 6.1.0.0 through 6.1.2.3 could allow an authenticated user to cause a denial of service due to uncontrolled resource consumption. IBM X-Force ID: 255827.	2024-02-09	6.5	CVE-2023-32341
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.8 and 6.1.0.0 through 6.1.2.3 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 265559.	2024-02-09	4.3	CVE-2023-42016
ibm -- storage_defender_resiliency_service	IBM Storage Defender - Resiliency Service 2.0 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 278748.	2024-02-10	5.5	CVE-2024-22312
if-so -- dynamic_content_personalization	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in If So Plugin If-So Dynamic Content Personalization allows Stored XSS.This issue affects If-So Dynamic Content Personalization: from n/a through 1.6.3.1.	2024-02-10	5.4	CVE-2023-51492
intel -- acat_software_maintained_by_intel(r)	Incorrect default permissions in some ACAT software maintained by Intel(R) before version 2.0.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-41231
intel -- intel(r)_battery_life_diagnostic_tool_software	Uncontrolled search path in some Intel(R) Battery Life Diagnostic Tool software before version 2.3.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-35060
intel -- intel(r)_binary_configuration_tool_software	Uncontrolled search path in some Intel(R) Binary Configuration Tool software before version 3.4.4 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-24591

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
intel -- intel(r)_c++_compiler_classic	Improper buffer restrictions in some Intel(R) C++ Compiler Classic before version 2021.8 may allow authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6	CVE-2023-29162
intel -- intel(r)_chipset_driver_software	Improper access control in some Intel(R) Chipset Driver Software before version 10.1.19444.8378 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-25174
intel -- intel(r)_chipset_driver_software	Incorrect default permissions in some Intel(R) Chipset Driver Software before version 10.1.19444.8378 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-28739
intel -- intel(r)_cip_software	Uncontrolled search path in some Intel(R) CIP software before version 2.4.10577 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-35769
intel -- intel(r)_dsa_software	Improper access control in some Intel(R) DSA software before version 23.4.33 may allow a privileged user to potentially enable escalation of privilege via local access.	2024-02-14	6.3	CVE-2023-35062
intel -- intel(r)_dsa_software	Improper access control in some Intel(R) DSA software before version 23.4.33 may allow an authenticated user to potentially enable denial of service via local access.	2024-02-14	5.5	CVE-2023-25073
intel -- intel(r)_ethernet_tools_and_driver_install_software	Insecure inherited permissions in some Intel(R) Ethernet tools and driver install software may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-33870
intel -- intel(r)_ethernet_tools_and_driver_install_software	Improper access control element in some Intel(R) Ethernet tools and driver install software, before versions 28.2, may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-39432
intel -- intel(r)_ispc_software	Uncontrolled search path in some Intel(R) ISPC software before version 1.21.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-38566
intel -- intel(r)_mas_software	Improper initialization in some Intel(R) MAS software before version 2.3 may allow an authenticated user to potentially enable denial of service via local access.	2024-02-14	5	CVE-2023-36490
intel -- intel(r)_mpi_library_software	Uncontrolled search path for some Intel(R) MPI Library Software before version 2021.11 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-41091
intel -- intel(r)_ofu_software	Protection mechanism failure in some Intel(R) OFU software before version 14.1.31 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-25945

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
intel -- intel(r)_oneapi_toolkit_and_component_software_installers	Uncontrolled search path in some Intel(R) oneAPI Toolkit and component software installers before version 4.3.2 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-32618
intel -- intel(r)_oneapi_toolkit_and_component_software_installers	Improper access control in some Intel(R) oneAPI Toolkit and component software installers before version 4.3.2 may allow an authenticated user to potentially enable denial of service via local access.	2024-02-14	5	CVE-2023-28715
intel -- intel(r)_optane(tm)_pmem_100_series_management_software	Improper access control in some Intel(R) Optane(TM) PMem 100 Series Management Software before version 01.00.00.3547 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-22311
intel -- intel(r)_optane(tm)_pmem_software	Improper access control in some Intel(R) Optane(TM) PMem software before versions 01.00.00.3547, 02.00.00.3915, 03.00.00.0483 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.6	CVE-2023-27517
intel -- intel(r)_pm_software	Improper authorization in some Intel(R) PM software may allow a privileged user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-38135
intel -- intel(r)_proset/wireless_and_intel(r)_killer(tm)_wi	Improper input validation for some Intel(R) PROSet/Wireless and Intel(R) Killer(TM) Wi-Fi software before version 22.240 may allow a privileged user to potentially enable escalation of privilege via local access.	2024-02-14	6	CVE-2023-25951
intel -- intel(r)_proset/wireless_and_intel(r)_killer(tm)_wi	Improper input validation for some Intel(R) PROSet/Wireless and Intel(R) Killer(TM) Wi-Fi software before version 22.240 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	2024-02-14	6.1	CVE-2023-28374
intel -- intel(r)_proset/wireless_and_intel(r)_killer(tm)_wi	Improper initialization for some Intel(R) PROSet/Wireless and Intel(R) Killer(TM) Wi-Fi software before version 22.240 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	2024-02-14	6.1	CVE-2023-28720
intel -- intel(r)_proset/wireless_and_intel(r)_killer(tm)_wi	Uncaught exception for some Intel(R) PROSet/Wireless and Intel(R) Killer(TM) Wi-Fi software before version 22.240 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	2024-02-14	4.3	CVE-2023-26586
intel -- intel(r)_proset/wireless_and_intel(r)_killer(tm)_wi	Insufficient adherence to expected conventions for some Intel(R) PROSet/Wireless and Intel(R) Killer(TM) Wi-Fi software before version 22.240 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	2024-02-14	4.3	CVE-2023-32642

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
intel -- intel(r)_proset/wireless_and_intel(r)_killer(tm)_wi	Protection mechanism failure for some Intel(R) PROSet/Wireless and Intel(R) Killer(TM) Wi-Fi software before version 22.240 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	2024-02-14	4.3	CVE-2023-32644
intel -- intel(r)_proset/wireless_and_intel(r)_killer(tm)_wi	Improper validation of specified type of input for some Intel(R) PROSet/Wireless and Intel(R) Killer(TM) Wi-Fi software before version 22.240 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	2024-02-14	4.3	CVE-2023-32651
intel -- intel(r)_proset/wireless_and_intel(r)_killer(tm)_wi	Improper input validation for some Intel(R) PROSet/Wireless and Intel(R) Killer(TM) Wi-Fi software before version 22.240 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	2024-02-14	4.3	CVE-2023-34983
intel -- intel(r)_proset/wireless_and_intel(r)_killer(tm)_wi	Improper initialization for some Intel(R) PROSet/Wireless and Intel(R) Killer(TM) Wi-Fi software before version 22.240 may allow an unauthenticated user to potentially enable information disclosure via adjacent access.	2024-02-14	4.3	CVE-2023-35061
intel -- intel(r)_qat_software_drivers_for_windows	Out-of-bounds read in some Intel(R) QAT software drivers for Windows before version QAT1.7-W-1.11.0 may allow an authenticated user to potentially enable denial of service via local access.	2024-02-14	6.5	CVE-2023-41252
intel -- intel(r)_qsfp+_configuration_utility_software	Uncontrolled search path in Intel(R) QSFP+ Configuration Utility software, all versions, may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-28745
intel -- intel(r)_sdk_for_opencl(tm)_applications_software	Uncontrolled search path in some Intel(R) SDK for OpenCL(TM) Applications software may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-36493
intel -- intel(r)_server_product_openbmc_firmware	Improper authentication in some Intel(R) Server Product OpenBMC firmware before version egs-1.09 may allow an authenticated user to enable escalation of privilege via local access.	2024-02-14	5.2	CVE-2023-31189
intel -- intel(r)_server_product_openbmc_firmware	Insufficiently protected credentials in some Intel(R) Server Product OpenBMC firmware before versions egs-1.05 may allow an unauthenticated user to enable information disclosure via network access.	2024-02-14	5.3	CVE-2023-32280
intel -- intel(r)_ssu_software	Uncontrolled search path element in some Intel(R) SSU software before version 3.0.0.2 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-40156

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
intel -- intel(r)_sur_for_gameplay_software	Uncontrolled search path in the Intel(R) SUR for Gameplay Software before version 2.0.1901 may allow a privileged user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-39932
intel -- intel(r)_sur_for_gameplay_software	Incorrect default permissions in the Intel(R) SUR for Gameplay Software before version 2.0.1901 may allow privileged user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-40154
intel -- intel(r)_thunderbolt(tm)_controllers_versions	Improper access control in firmware for some Intel(R) Thunderbolt(TM) Controllers versions before 41 may allow a privileged user to enable denial of service via local access.	2024-02-14	6.1	CVE-2023-28396
intel -- intel(r)_thunderbolt(tm)_dch_drivers_for_windows	Improper buffer restrictions in some Intel(R) Thunderbolt(TM) DCH drivers for Windows before version 88 may allow an authenticated user to potentially enable information disclosure via local access.	2024-02-14	6.5	CVE-2023-22390
intel -- intel(r)_thunderbolt(tm)_dch_drivers_for_windows	Improper access control in some Intel(R) Thunderbolt(TM) DCH drivers for Windows before version 88 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.3	CVE-2023-24481
intel -- intel(r)_thunderbolt(tm)_dch_drivers_for_windows	Unquoted search path or element in some Intel(R) Thunderbolt(TM) DCH drivers for Windows before version 88 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-24542
intel -- intel(r)_thunderbolt(tm)_dch_drivers_for_windows	Improper buffer restrictions in some Intel(R) Thunderbolt(TM) DCH drivers for Windows before version 88 may allow a privileged user to potentially enable escalation of privilege via local access.	2024-02-14	6.1	CVE-2023-24589
intel -- intel(r)_thunderbolt(tm)_dch_drivers_for_windows	Uncontrolled search path element in some Intel(R) Thunderbolt(TM) DCH drivers for Windows before version 88 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-25779
intel -- intel(r)_thunderbolt(tm)_dch_drivers_for_windows	Improper access control in some Intel(R) Thunderbolt(TM) DCH drivers for Windows before version 88 may allow an authenticated user to potentially enable denial of service via local access.	2024-02-14	5.5	CVE-2023-22848
intel -- intel(r)_thunderbolt(tm)_dch_drivers_for_windows	Uncontrolled resource consumption in some Intel(R) Thunderbolt(TM) DCH drivers for Windows before version 88 may allow an authenticated user to potentially enable denial of service via local access.	2024-02-14	5.5	CVE-2023-25769
intel -- intel(r)_thunderbolt(tm)_dch_drivers_	Improper access control in some Intel(R) Thunderbolt(TM) DCH drivers for Windows before version 88 may allow an authenticated user to potentially enable denial of service via local access.	2024-02-14	5	CVE-2023-26585

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
for_windows				
intel -- intel(r)_thunderbolt(tm)_dch_drivers_for_windows	Improper input validation in some Intel(R) Thunderbolt(TM) DCH drivers for Windows before version 88 may allow an unauthenticated user to potentially enable information disclosure via adjacent access.	2024-02-14	4.3	CVE-2023-24463
intel -- intel(r)_thunderbolt(tm)_dch_drivers_for_windows	Improper access control in some Intel(R) Thunderbolt(TM) DCH drivers for Windows before version 88 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	4.2	CVE-2023-27301
intel -- intel(r)_thunderbolt(tm)_dch_drivers_for_windows	Improper buffer restrictions in some Intel(R) Thunderbolt(TM) DCH drivers for Windows before version 88 may allow a privileged user to potentially enable escalation of privilege via local access.	2024-02-14	4.6	CVE-2023-27308
intel -- intel(r)_vroc_software	Improper access control in some Intel(R) VROC software before version 8.0.8.1001 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-31271
intel -- intel(r)_vroc_software	Uncontrolled search path element in some Intel(R) VROC software before version 8.0.8.1001 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-32646
intel -- intel(r)_vroc_software	Incorrect default permissions in some Intel(R) VROC software before version 8.0.8.1001 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-34315
intel -- intel(r)_vroc_software	Path transversal in some Intel(R) VROC software before version 8.0.8.1001 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-35003
intel -- intel(r)_xtu_software	Uncontrolled search path in some Intel(R) XTU software before version 7.12.0.29 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.7	CVE-2023-28407
intel -- intel(r)_xtu_software	Improper access control in some Intel(R) XTU software before version 7.12.0.29 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.8	CVE-2023-32647
intel -- intel(r)_xtu_software	Improper access control in some Intel(R) XTU software before version 7.12.0.29 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	5.5	CVE-2023-38561
intel -- intel_unite(r)_client_software	Improper access control in some Intel Unite(R) Client software before version 4.2.35041 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	6.6	CVE-2023-40161

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
intel -- sps_firmware	Uncontrolled resource consumption for some Intel(R) SPS firmware before version SPS_E5_06.01.04.002.0 may allow a privileged user to potentially enable denial of service via network access.	2024-02-14	4.9	CVE-2023-29153
intel -- tensorflow	Improper buffer restrictions in Intel(R) Optimization for TensorFlow before version 2.13.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-02-14	5.5	CVE-2023-30767
internallinkjuicer -- internal_link_juicer	The Internal Link Juicer: SEO Auto Linker for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings such as 'ilj_settings_field_links_per_page' in all versions up to, and including, 2.23.4 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.	2024-02-09	4.8	CVE-2024-0657
isc -- bind_9	If a resolver cache has a very large number of ECS records stored for the same name, the process of cleaning the cache database node for this name can significantly impair query performance. This issue affects BIND 9 versions 9.11.3-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.45-S1, and 9.18.11-S1 through 9.18.21-S1.	2024-02-13	5.3	CVE-2023-5680
jboss -- undertow	A path traversal vulnerability was found in Undertow. This issue may allow a remote attacker to append a specially crafted sequence to an HTTP request for an application deployed to JBoss EAP, which may permit access to privileged or restricted files and directories.	2024-02-12	5.3	CVE-2024-1459
jwcrypto -- jwcrypto	A vulnerability was found in JWCrypto. This flaw allows an attacker to cause a denial of service (DoS) attack and possible password brute-force and dictionary attacks to be more resource-intensive. This issue can result in a large amount of computational consumption, causing a denial-of-service attack.	2024-02-12	5.3	CVE-2023-6681
kalli_dan -- kd_coming_soon	Deserialization of Untrusted Data vulnerability in Kalli Dan. KD Coming Soon. This issue affects KD Coming Soon: from n/a through 1.7.	2024-02-12	5.4	CVE-2023-46615
leap13 -- premium_addons_for_elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Leap13 Premium Addons for Elementor allows Stored XSS.This issue affects Premium Addons for Elementor: from n/a through 4.10.16.	2024-02-10	5.4	CVE-2024-24831
linksys -- wrt54gl_firmware	A vulnerability was found in Linksys WRT54GL 4.30.18. It has been classified as problematic. This affects an unknown part of the file /wlaninfo.htm of the component Web Management Interface. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. The identifier VDB-253329 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-10	4.3	CVE-2024-1405
linksys -- wrt54gl_firmware	A vulnerability was found in Linksys WRT54GL 4.30.18. It has been declared as problematic. This vulnerability affects unknown code of the file /SysInfo1.htm of the component Web Management Interface. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. VDB-253330 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-10	4.3	CVE-2024-1406
linux -- kernel	A vulnerability was reported in the Open vSwitch sub-component in the Linux Kernel. The flaw occurs when a recursive operation of code push recursively calls into the code block. The OVS module does not validate the stack depth, pushing too many frames and causing a stack overflow. As a result, this can lead to a crash or other related issues.	2024-02-11	5.5	CVE-2024-1151

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux	A flaw was found in the decompression function of registry-support. This issue can be triggered if an unauthenticated remote attacker tricks a user into opening a specially modified .tar archive, leading to the cleanup process following relative paths to overwrite or delete files outside the intended scope.	2024-02-14	6.8	CVE-2024-1485
logichunt -- owl_carousel	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LogicHunt OWL Carousel - WordPress Owl Carousel Slider allows Stored XSS.This issue affects OWL Carousel - WordPress Owl Carousel Slider: from n/a through 1.4.0.	2024-02-10	5.4	CVE-2024-24801
mastodon -- mastodon	Mastodon is a free, open-source social network server based on ActivityPub. Mastodon allows new identities from configured authentication providers (CAS, SAML, OIDC) to attach to existing local users with the same e-mail address. This results in a possible account takeover if the authentication provider allows changing the e-mail address or multiple authentication providers are configured. When a user logs in through an external authentication provider for the first time, Mastodon checks the e-mail address passed by the provider to find an existing account. However, using the e-mail address alone means that if the authentication provider allows changing the e-mail address of an account, the Mastodon account can immediately be hijacked. All users logging in through external authentication providers are affected. The severity is medium, as it also requires the external authentication provider to misbehave. However, some well-known OIDC providers (like Microsoft Azure) make it very easy to accidentally allow unverified e-mail changes. Moreover, OpenID Connect also allows dynamic client registration. This issue has been addressed in versions 4.2.6, 4.1.14, 4.0.14, and 3.5.18. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-14	4.2	CVE-2024-25618
mattermost -- mattermost_server	Mattermost fails to check if a custom emoji reaction exists when sending it to a post and to limit the amount of custom emojis allowed to be added in a post, allowing an attacker sending a huge amount of non-existent custom emojis in a post to crash the mobile app of a user seeing the post.	2024-02-09	4.3	CVE-2024-1402
mattermost -- mattermost_server	Mattermost Jira Plugin handling subscriptions fails to check the security level of an incoming issue or limit it based on the user who created the subscription resulting in registered users on Jira being able to create webhooks that give them access to all Jira issues.	2024-02-09	4.1	CVE-2024-24774
mattermost -- mattermost_server	Mattermost fails to check the required permissions in the POST /api/v4/channels/stats/member_count API resulting in channel member counts being leaked to a user without permissions.	2024-02-09	4.3	CVE-2024-24776
mediawiki -- managewiki	ManageWiki is a MediaWiki extension allowing users to manage wikis. Special:ManageWiki does not escape escape interface messages on the `columns` and `help` keys on the form descriptor. An attacker may exploit this and would have a cross site scripting attack vector. Exploiting this on-wiki requires the `(editinterface)` right. Users should apply the code changes in commits `886cc6b94`, `2ef0f50880`, and `6942e8b2c` to resolve this vulnerability. There are no known workarounds for this vulnerability.	2024-02-09	6.5	CVE-2024-25109
microsoft -- azure_file_sync	Microsoft Azure File Sync Elevation of Privilege Vulnerability	2024-02-13	5.3	CVE-2024-21397
microsoft -- azure_stack_hub	Azure Stack Hub Spoofing Vulnerability	2024-02-13	6.5	CVE-2024-20679
microsoft -- entra	Microsoft Azure Active Directory B2C Spoofing Vulnerability	2024-02-13	6.8	CVE-2024-21381
microsoft -- microsoft_teams_f	Microsoft Teams for Android Information Disclosure	2024-02-13	5	CVE-2024-21374

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
or_android				
microsoft -- skype_for_business_server_2019_cu7	Skype for Business Information Disclosure Vulnerability	2024-02-13	5.7	CVE-2024-20695
microsoft -- windows_10_version_1809	Windows USB Generic Parent Driver Remote Code Execution Vulnerability	2024-02-13	6.4	CVE-2024-21339
microsoft -- windows_10_version_1809	Windows Kernel Remote Code Execution Vulnerability	2024-02-13	6.8	CVE-2024-21341
microsoft -- windows_10_version_1809	Windows Lightweight Directory Access Protocol (LDAP) Denial of Service Vulnerability	2024-02-13	6.5	CVE-2024-21356
microsoft -- windows_10_version_1809	Windows Network Address Translation (NAT) Denial of Service Vulnerability	2024-02-13	5.9	CVE-2024-21343
microsoft -- windows_10_version_1809	Windows Network Address Translation (NAT) Denial of Service Vulnerability	2024-02-13	5.9	CVE-2024-21344
microsoft -- windows_10_version_1809	Windows Kernel Security Feature Bypass Vulnerability	2024-02-13	5.5	CVE-2024-21362
microsoft -- windows_10_version_1809	Trusted Compute Base Elevation of Privilege Vulnerability	2024-02-13	4.1	CVE-2024-21304
microsoft -- windows_10_version_1809	Windows Kernel Information Disclosure Vulnerability	2024-02-13	4.6	CVE-2024-21340
microsoft -- windows_server_2022	Windows Hyper-V Denial of Service Vulnerability	2024-02-13	6.5	CVE-2024-20684
mitsubishi_electric_corporation -- melsec_iq-r_series_safety_cpu_r08sfcpu	Incorrect Privilege Assignment vulnerability in Mitsubishi Electric Corporation MELSEC iQ-R Series Safety CPU R08/16/32/120SFCPU all versions and MELSEC iQ-R Series SIL2 Process CPU R08/16/32/120PSFCPU all versions allow a remote authenticated attacker who has logged into the product as a non-administrator user to disclose the credentials (user ID and password) of a user with a lower access level than the attacker by sending a specially crafted packet.	2024-02-13	6.5	CVE-2023-6815

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
moodle -- lms	Inadequate access control in Moodle LMS. This vulnerability could allow a local user with a student role to create arbitrary events intended for users with higher roles. It could also allow the attacker to add events to the calendar of all users without their prior consent.	2024-02-12	6.5	CVE-2024-1439
netapp -- snapcenter	SnapCenter versions 4.8 prior to 5.0 are susceptible to a vulnerability which could allow an authenticated SnapCenter Server user to modify system logging configuration settings	2024-02-16	5.4	CVE-2024-21987
netapp -- storagegrid	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.8 are susceptible to a Denial of Service (DoS) vulnerability. Successful exploit by an authenticated attacker could lead to an out of memory condition or node reboot.	2024-02-16	6.5	CVE-2024-21983
netapp -- storagegrid	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.8 are susceptible to a difficult to exploit Reflected Cross-Site Scripting (XSS) vulnerability. Successful exploit requires the attacker to know specific information about the target instance and trick a privileged user into clicking a specially crafted link. This could allow the attacker to view or modify configuration settings or add or modify user accounts.	2024-02-16	5.9	CVE-2024-21984
netgear -- r7000_firmware	A vulnerability has been found in Netgear R7000 1.0.11.136_10.2.120 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /currentsetting.htm of the component Web Management Interface. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. The identifier VDB-253381 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-11	6.5	CVE-2024-1430
netgear -- r7000_firmware	A vulnerability was found in Netgear R7000 1.0.11.136_10.2.120 and classified as problematic. Affected by this issue is some unknown functionality of the file /debuginfo.htm of the component Web Management Interface. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. VDB-253382 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-11	6.5	CVE-2024-1431
nicdark -- restaurant_reservations	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nicdark Restaurant Reservations allows Stored XSS.This issue affects Restaurant Reservations: from n/a through 1.8.	2024-02-12	6.5	CVE-2023-51403
ninjateam -- wp_chat_app	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NinjaTeam WP Chat App allows Stored XSS. This issue affects WP Chat App: from n/a through 3.4.4.	2024-02-12	5.9	CVE-2023-51370
nodejs -- undici	Undici is an HTTP/1.1 client, written from scratch for Node.js. In affected versions calling `fetch(url)` and not consuming the incoming body ((or consuming it very slowing) will lead to a memory leak. This issue has been addressed in version 6.6.1. Users are advised to upgrade. Users unable to upgrade should make sure to always consume the incoming body.	2024-02-16	6.5	CVE-2024-24750
open-xchange_gmbh -- ox_app_suite	User ID references at mentions in document comments were not correctly sanitized. Script code could be injected to a user's session when working with a malicious document. Please deploy the provided updates and patch releases. User-defined content like comments and mentions are now filtered to avoid potentially malicious content. No publicly available exploits are known.	2024-02-12	6.1	CVE-2023-41703
open-xchange_gmbh -- ox_app_suite	Processing of user-defined DAV user-agent strings is not limited. Availability of OX App Suite could be reduced due to high processing load. Please deploy the provided updates and patch releases. Processing time of DAV user-agents now gets monitored, and the related request is terminated if a resource threshold is reached. No publicly available exploits are known.	2024-02-12	6.5	CVE-2023-41705

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
open-xchange_gmbh -- ox_app_suite	Processing time of drive search expressions now gets monitored, and the related request is terminated if a resource threshold is reached. Availability of OX App Suite could be reduced due to high processing load. Please deploy the provided updates and patch releases. Processing of user-defined drive search expressions is not limited No publicly available exploits are known.	2024-02-12	6.5	CVE-2023-41706
open-xchange_gmbh -- ox_app_suite	Processing of user-defined mail search expressions is not limited. Availability of OX App Suite could be reduced due to high processing load. Please deploy the provided updates and patch releases. Processing time of mail search expressions now gets monitored, and the related request is terminated if a resource threshold is reached. No publicly available exploits are known.	2024-02-12	6.5	CVE-2023-41707
open-xchange_gmbh -- ox_app_suite	References to the "app loader" functionality could contain redirects to unexpected locations. Attackers could forge app references that bypass existing safeguards to inject malicious script code. Please deploy the provided updates and patch releases. References to apps are now more strictly controlled to avoid relative references. No publicly available exploits are known.	2024-02-12	5.4	CVE-2023-41708
oracle_corporation -- application_object_library	Vulnerability in the Oracle Application Object Library product of Oracle E-Business Suite (component: DB Privileges). 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 Application Object Library. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Object Library accessible data as well as unauthorized read access to a subset of Oracle Application Object Library accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2024-02-17	6.5	CVE-2024-20929
oracle_corporation -- application_object_library	Vulnerability in the Oracle Application Object Library product of Oracle E-Business Suite (component: Login - SSO). 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 Application Object Library. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Application Object Library. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2024-02-17	5.3	CVE-2024-20915
oracle_corporation -- bi_publisher_(formerly_xml_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 and 7.0.0.0.0. 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).	2024-02-17	5.4	CVE-2024-20980
oracle_corporation -- business_intelligence_enterprise_edition	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: BI Platform Security). 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 Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and 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 update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4	2024-02-17	5.4	CVE-2024-20913

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(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).			
oracle_corporation -- common_applications	Vulnerability in the Oracle Common Applications product of Oracle E-Business Suite (component: CRM User Management Framework). 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 Common Applications. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Applications, 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 Common Applications accessible data as well as unauthorized read access to a subset of Oracle Common Applications 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).	2024-02-17	5.4	CVE-2024-20947
oracle_corporation -- crm_technical_foundation	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Admin Console). 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 CRM Technical Foundation. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle CRM Technical Foundation. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	2024-02-17	4.3	CVE-2024-20939
oracle_corporation -- 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).	2024-02-17	6.1	CVE-2024-20949
oracle_corporation -- 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).	2024-02-17	6.1	CVE-2024-20951
oracle_corporation -- database_-_enterprise_edition	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19.3-19.21 and 21.3-21.12. Easily exploitable vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via Oracle Net to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java VM accessible data. CVSS 3.1 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N).	2024-02-17	6.5	CVE-2024-20903

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle_corporation -- 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).	2024-02-17	6.1	CVE-2024-20933
oracle_corporation -- 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).	2024-02-17	6.1	CVE-2024-20935
oracle_corporation -- installed_base	Vulnerability in the Oracle Installed Base product of Oracle E-Business Suite (component: HTML UI). 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).	2024-02-17	6.1	CVE-2024-20941
oracle_corporation -- 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 low privileged 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 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).	2024-02-17	5.4	CVE-2024-20958
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. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service.	2024-02-17	5.9	CVE-2024-20919

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CVSS 3.1 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).			
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 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).	2024-02-17	5.9	CVE-2024-20921
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: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition executes 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 4.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N).	2024-02-17	4.7	CVE-2024-20945
oracle_corporation -- jd_edwards_enterpriseone_tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Monitoring and Diagnostics SEC). Supported versions that are affected are Prior to 9.2.8.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2024-02-17	4.3	CVE-2024-20937
oracle_corporation -- knowledge_management	Vulnerability in the Oracle Knowledge Management 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 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 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).	2024-02-17	5.4	CVE-2024-20943

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle_corporation -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: RAPID). 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).	2024-02-17	6.5	CVE-2024-20960
oracle_corporation -- mysql_server	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).	2024-02-17	6.5	CVE-2024-20962
oracle_corporation -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Difficult to exploit 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 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	2024-02-17	5.3	CVE-2024-20964
oracle_corporation -- mysql_server	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).	2024-02-17	4.9	CVE-2024-20966
oracle_corporation -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Difficult to exploit 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 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-02-17	4.4	CVE-2024-20968
oracle_corporation -- mysql_server	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).	2024-02-17	4.9	CVE-2024-20970
oracle_corporation -- mysql_server	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	2024-02-17	4.9	CVE-2024-20972

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).			
oracle_corporation -- mysql_server	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).	2024-02-17	4.9	CVE-2024-20974
oracle_corporation -- mysql_server	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).	2024-02-17	4.9	CVE-2024-20976
oracle_corporation -- mysql_server	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).	2024-02-17	4.9	CVE-2024-20978
oracle_corporation -- mysql_server	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).	2024-02-17	4.9	CVE-2024-20982
oracle_corporation -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server : Security : Firewall). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Difficult to exploit 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 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2024-02-17	4.4	CVE-2024-20984
oracle_corporation -- sun_zfs_storage_appliance_kit_(ak)_software	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Object Store). The supported version that is affected is 8.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP 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 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2024-02-17	4.3	CVE-2023-21833
oracle_corporation -- web_applications_desktop_integrator	Vulnerability in the Oracle Web Applications Desktop Integrator product of Oracle E-Business Suite (component: File download). 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 Web Applications Desktop Integrator. Successful attacks require human interaction from a person other than	2024-02-17	6.1	CVE-2024-20907

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the attacker and while the vulnerability is in Oracle Web Applications Desktop Integrator, 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 Web Applications Desktop Integrator accessible data as well as unauthorized read access to a subset of Oracle Web Applications Desktop Integrator 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_corporation -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, 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 WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server 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).	2024-02-17	6.1	CVE-2024-20986
otwthemes -- buttons_shortcode_and_widget	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in OTWthemes.Com Buttons Shortcode and Widget allows Stored XSS.This issue affects Buttons Shortcode and Widget: from n/a through 1.16.	2024-02-12	5.4	CVE-2024-24930
palo_alto_networks -- pan-os	A cross-site scripting (XSS) vulnerability in Palo Alto Networks PAN-OS software enables a malicious authenticated read-write administrator to store a JavaScript payload using the web interface on Panorama appliances. This enables the impersonation of another authenticated administrator.	2024-02-14	6.8	CVE-2024-0007
palo_alto_networks -- pan-os	Web sessions in the management interface in Palo Alto Networks PAN-OS software do not expire in certain situations, making it susceptible to unauthorized access.	2024-02-14	6.6	CVE-2024-0008
palo_alto_networks -- pan-os	An improper verification vulnerability in the GlobalProtect gateway feature of Palo Alto Networks PAN-OS software enables a malicious user with stolen credentials to establish a VPN connection from an unauthorized IP address.	2024-02-14	6.3	CVE-2024-0009
palo_alto_networks -- pan-os	A reflected cross-site scripting (XSS) vulnerability in the GlobalProtect portal feature of Palo Alto Networks PAN-OS software enables execution of malicious JavaScript (in the context of a user's browser) if a user clicks on a malicious link, allowing phishing attacks that could lead to credential theft.	2024-02-14	4.3	CVE-2024-0010
palo_alto_networks -- pan-os	A reflected cross-site scripting (XSS) vulnerability in the Captive Portal feature of Palo Alto Networks PAN-OS software enables execution of malicious JavaScript (in the context of an authenticated Captive Portal user's browser) if a user clicks on a malicious link, allowing phishing attacks that could lead to credential theft.	2024-02-14	4.3	CVE-2024-0011
photoboxone -- smtp_mail	Cross-Site Request Forgery (CSRF) vulnerability in Photoboxone SMTP Mail. This issue affects SMTP Mail: from n/a through 1.3.20.	2024-02-13	4.3	CVE-2024-25914
pluginus -- woot	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in realmag777 Active Products Tables for WooCommerce. Professional products tables for WooCommerce store allows Stored XSS.This issue affects Active Products Tables for WooCommerce. Professional products tables for WooCommerce store : from n/a through 1.0.6.	2024-02-10	5.4	CVE-2023-51480
pquic -- pquic	In PQUIC before 5bde5bb, retention of unused initial encryption keys allows attackers to disrupt a connection with a PSK configuration by sending a	2024-02-09	6.5	CVE-2024-25679

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CONNECTION_CLOSE frame that is encrypted via the initial key computed. Network traffic sniffing is needed as part of exploitation.			
prasidhdamalla -- honeypot_for_wp_comment	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Prasidhda Malla Honeypot for WP Comment allows Reflected XSS. This issue affects Honeypot for WP Comment: from n/a through 2.2.3.	2024-02-12	6.1	CVE-2024-24933
python -- python	nonebot2 is a cross-platform Python asynchronous chatbot framework written in Python. This security advisory pertains to a potential information leak (e.g., environment variables) in instances where developers utilize `MessageTemplate` and incorporate user-provided data into templates. The identified vulnerability has been remedied in pull request #2509 and will be included in versions released from 2.2.0. Users are strongly advised to upgrade to these patched versions to safeguard against the vulnerability. A temporary workaround involves filtering underscores before incorporating user input into the message template.	2024-02-09	6.5	CVE-2024-21624
qnap_systems_inc -- qts	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.5.2645 build 20240116 and later QuTS hero h5.1.5.2647 build 20240118 and later QuTScloud c5.1.5.2651 and later	2024-02-13	5.8	CVE-2023-47218
qnap_systems_inc -- qts	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.5.2645 build 20240116 and later QTS 4.5.4.2627 build 20231225 and later QTS 4.3.6.2665 build 20240131 and later QTS 4.3.4.2675 build 20240131 and later QTS 4.3.3.2644 build 20240131 and later QTS 4.2.6 build 20240131 and later QuTS hero h5.1.5.2647 build 20240118 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later	2024-02-13	5.8	CVE-2023-50358
red_hat -- 389-ds-base	A heap overflow flaw was found in 389-ds-base. This issue leads to a denial of service when writing a value larger than 256 chars in log_entry_attr.	2024-02-12	5.5	CVE-2024-1062
red_hat -- openshift	A flaw was found in OpenShift. The existing Cross-Site Request Forgery (CSRF) protections in place do not properly protect GET requests, allowing for the creation of WebSockets via CSRF.	2024-02-16	5.4	CVE-2024-1342
ryan_duff_peter_westwood -- wp_contact_form	Cross-Site Request Forgery (CSRF) vulnerability in Ryan Duff, Peter Westwood WP Contact Form. This issue affects WP Contact Form: from n/a through 1.6.	2024-02-12	4.3	CVE-2024-24929
sametime -- sametime	Sametime is impacted by sensitive fields with autocomplete enabled in the Legacy web chat client. By default, this allows user entered data to be stored by the browser.	2024-02-10	4	CVE-2023-45696
sametime -- sametime	Sametime is impacted by lack of clickjacking protection in Outlook add-in. The application is not implementing appropriate protections in order to protect users from clickjacking attacks.	2024-02-10	4.8	CVE-2023-45698
sap_se -- sap_bam_(bank_account_management)	SAP Bank Account Management (BAM) allows an authenticated user with restricted access to use functions which can result in escalation of privileges with low impact on confidentiality, integrity and availability of the application.	2024-02-13	6.3	CVE-2024-24739
sap_se -- sap_companion	SAP Companion - version <3.1.38, has a URL with parameter that could be vulnerable to XSS attack. The attacker could send a malicious link to a user that	2024-02-13	5.4	CVE-2024-22129

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	would possibly allow an attacker to retrieve the sensitive information and cause minor impact on the integrity of the web application.			
sap_se -- sap_crm_(webclient_ui)	SAP CRM WebClient UI - version S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An attacker with low privileges can cause limited impact to integrity of the application data after successful exploitation. There is no impact on confidentiality and availability.	2024-02-13	4.1	CVE-2024-24742
sap_se -- sap_fiori_app_(my_overtime_requests)	The SAP Fiori app (My Overtime Request) - version 605, does not perform the necessary authorization checks for an authenticated user which may result in an escalation of privileges. It is possible to manipulate the URLs of data requests to access information that the user should not have access to. There is no impact on integrity and availability.	2024-02-13	4.3	CVE-2024-25643
sap_se -- sap_master_data_governance_material	SAP Master Data Governance for Material Data - versions 618, 619, 620, 621, 622, 800, 801, 802, 803, 804, does not perform necessary authorization check for an authenticated user, resulting in escalation of privileges. This could allow an attacker to read some sensitive information but no impact to integrity and availability.	2024-02-13	4.3	CVE-2024-24741
sap_se -- sap_netweaver_application_server_abap_(sap_kernel)	SAP NetWeaver Application Server (ABAP) - versions KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, KERNEL 7.85, KERNEL 7.89, KERNEL 7.93, KERNEL 7.94, KRNL64UC 7.53, under certain conditions, allows an attacker to access information which could otherwise be restricted with low impact on confidentiality of the application.	2024-02-13	5.3	CVE-2024-24740
sap_se -- sap_netweaver_business_client_for_html	SAP NWBC for HTML - versions SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, SAP_UI 758, SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An unauthenticated attacker can inject malicious javascript to cause limited impact to confidentiality and integrity of the application data after successful exploitation.	2024-02-13	4.7	CVE-2024-22128
sentry -- sentry	Sentry is an error tracking and performance monitoring platform. Sentry's integration platform provides a way for external services to interact with Sentry. One of such integrations, the Phabricator integration (maintained by Sentry) with version <=24.1.1 contains a constrained SSRF vulnerability. An attacker could make Sentry send POST HTTP requests to arbitrary URLs (including internal IP addresses) by providing an unsanitized input to the Phabricator integration. However, the body payload is constrained to a specific format. If an attacker has access to a Sentry instance, this allows them to: 1. interact with internal network; 2. scan local/remote ports. This issue has been fixed in Sentry self-hosted release 24.1.2, and has already been mitigated on sentry.io on February 8. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-09	5.3	CVE-2024-24829
siemens -- openpcs_7_v9.1	A vulnerability has been identified in OpenPCS 7 V9.1 (All versions), SIMATIC BATCH V9.1 (All versions), SIMATIC PCS 7 V9.1 (All versions), SIMATIC Route Control V9.1 (All versions), SIMATIC WinCC Runtime Professional V18 (All versions), SIMATIC WinCC Runtime Professional V19 (All versions), SIMATIC WinCC V7.4 (All versions), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 15), SIMATIC WinCC V8.0 (All versions < V8.0 SP4). The implementation of the RPC (Remote Procedure call) communication protocol in the affected products do not properly handle certain unorganized RPC messages. An attacker could use this vulnerability to cause a denial of service condition in the RPC server.	2024-02-13	6.5	CVE-2023-48363
siemens -- openpcs_7_v9.1	A vulnerability has been identified in OpenPCS 7 V9.1 (All versions), SIMATIC BATCH V9.1 (All versions), SIMATIC PCS 7 V9.1 (All versions), SIMATIC Route Control V9.1 (All versions), SIMATIC WinCC Runtime Professional V18 (All versions), SIMATIC WinCC Runtime Professional V19 (All versions), SIMATIC WinCC V7.4 (All	2024-02-13	6.5	CVE-2023-48364

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	versions), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 15), SIMATIC WinCC V8.0 (All versions < V8.0 SP4). The implementation of the RPC (Remote Procedure call) communication protocol in the affected products do not properly handle certain malformed RPC messages. An attacker could use this vulnerability to cause a denial of service condition in the RPC server.			
siemens -- tecnomatix_plant_simulation	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions), Tecnomatix Plant Simulation V2302 (All versions < V2302.0007). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted SPP files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	2024-02-13	5.5	CVE-2024-23799
siemens -- tecnomatix_plant_simulation	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions), Tecnomatix Plant Simulation V2302 (All versions < V2302.0007). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted SPP files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	2024-02-13	5.5	CVE-2024-23800
siemens -- tecnomatix_plant_simulation	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions), Tecnomatix Plant Simulation V2302 (All versions < V2302.0007). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted SPP files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	2024-02-13	5.5	CVE-2024-23801
silabs.com -- gsdk	A memory leak in the Silicon Labs' Bluetooth stack for EFR32 products may cause memory to be exhausted when sending notifications to multiple clients, this results in all Bluetooth operations, such as advertising and scanning, to stop.	2024-02-15	6.5	CVE-2024-0240
squid-cache -- squid	Squid is an open-source caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. Due to a Collapse of Data into Unsafe Value bug ,Squid may be vulnerable to a Denial of Service attack against HTTP header parsing. This problem allows a remote client or a remote server to perform Denial of Service when sending oversized headers in HTTP messages. In versions of Squid prior to 6.5 this can be achieved if the request_header_max_size or reply_header_max_size settings are unchanged from the default. In Squid version 6.5 and later, the default setting of these parameters is safe. Squid will emit a critical warning in cache.log if the administrator is setting these parameters to unsafe values. Squid will not at this time prevent these settings from being changed to unsafe values. Users are advised to upgrade to version 6.5. There are no known workarounds for this vulnerability. This issue is also tracked as SQUID-2024:2	2024-02-14	5.3	CVE-2024-25617
svix -- svix	Versions of the package svix before 1.17.0 are vulnerable to Authentication Bypass due to an issue in the verify function where signatures of different lengths are incorrectly compared. An attacker can bypass signature verification by providing a shorter signature that matches the beginning of the actual signature. **Note:** The attacker would need to know a victim uses the Rust library for verification, no easy way to automatically check that; and uses webhooks by a service that uses Svix, and then figure out a way to craft a malicious payload that will actually include all of the correct identifiers needed to trick the receivers to cause actual issues.	2024-02-13	6.8	CVE-2024-21491
swadeshswain -- before_after_image_slider	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in swadeshswain Before After Image Slider WP allows Stored XSS.This issue affects Before After Image Slider WP: from n/a through 2.2.	2024-02-12	5.4	CVE-2024-24931
task_manager_in_php_with_source_code_project -- task_manager_in_php_with_source_code	A cross-site scripting (XSS) vulnerability in Task Manager App v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Project Name parameter /TaskManager/Projects.php.	2024-02-14	6.1	CVE-2024-25218

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
task_manager_in_php_with_source_code_project -- task_manager_in_php_with_source_code	A cross-site scripting (XSS) vulnerability in Task Manager App v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Task Name parameter /TaskManager/Task.php.	2024-02-14	6.1	CVE-2024-25219
task_manager_in_php_with_source_code_project -- task_manager_in_php_with_source_code	A cross-site scripting (XSS) vulnerability in Task Manager App v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Note Section parameter at /TaskManager/Tasks.php.	2024-02-14	6.1	CVE-2024-25221
tenable -- security_center	An HTML injection vulnerability exists where an authenticated, remote attacker with administrator privileges on the Security Center application could modify Repository parameters, which could lead to HTML redirection attacks.	2024-02-14	5.9	CVE-2024-1471
treasure-data -- digdag	Digdag is an open source tool that to build, run, schedule, and monitor complex pipelines of tasks across various platforms. Treasure Data's digdag workload automation system is susceptible to a path traversal vulnerability if it's configured to store log files locally. This issue may lead to information disclosure and has been addressed in release version 0.10.5.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-14	5.3	CVE-2024-25125
trellix -- trellix_central_management_(cm)	A cross-site scripting vulnerability in Trellix Central Management (CM) prior to 9.1.3.97129 allows a remote authenticated attacker to craft CM dashboard internal requests causing arbitrary content to be injected into the response when accessing the CM dashboard.	2024-02-13	4.6	CVE-2023-6072
typo3 -- typo3	TYPO3 is an open-source PHP based web content management system released under the GNU GPL. Password hashes were being reflected in the editing forms of the TYPO3 backend user interface. This allowed attackers to crack the plaintext password using brute force techniques. Exploiting this vulnerability requires a valid backend user account. Users are advised to update to TYPO3 versions 8.7.57 ELTS, 9.5.46 ELTS, 10.4.43 ELTS, 11.5.35 LTS, 12.4.11 LTS, 13.0.1 that fix the problem described. There are no known workarounds for this issue.	2024-02-13	4.3	CVE-2024-25118
typo3 -- typo3	TYPO3 is an open source PHP based web content management system released under the GNU GPL. The plaintext value of `$GLOBALS['SYS']['encryptionKey']` was displayed in the editing forms of the TYPO3 Install Tool user interface. This allowed attackers to utilize the value to generate cryptographic hashes used for verifying the authenticity of HTTP request parameters. Exploiting this vulnerability requires an administrator-level backend user account with system maintainer permissions. Users are advised to update to TYPO3 versions 8.7.57 ELTS, 9.5.46 ELTS, 10.4.43 ELTS, 11.5.35 LTS, 12.4.11 LTS, 13.0.1 that fix the problem described. There are no known workarounds for this vulnerability.	2024-02-13	4.9	CVE-2024-25119
typo3 -- typo3	TYPO3 is an open-source PHP based web content management system released under the GNU GPL. The TYPO3-specific `t3://` URI scheme could be used to access resources outside of the users' permission scope. This encompassed files, folders, pages, and records (although only if a valid link-handling configuration was provided). Exploiting this vulnerability requires a valid backend user account. Users are advised to update to TYPO3 versions 8.7.57 ELTS, 9.5.46 ELTS, 10.4.43 ELTS, 11.5.35 LTS, 12.4.11 LTS, 13.0.1 that fix the problem described. There are no known workarounds for this issue.	2024-02-13	4.3	CVE-2024-25120
virusblokada -- vba32_antivirus	Vba32 Antivirus v3.36.0 is vulnerable to an Arbitrary Memory Read vulnerability by triggering the 0x22201B, 0x22201F, 0x222023, 0x222027 ,0x22202B, 0x22202F, 0x22203F, 0x222057 and 0x22205B IOCTL codes of the Vba32m64.sys driver.	2024-02-13	6.3	CVE-2024-23439

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
virusblokada -- vba32_antivirus	Vba32 Antivirus v3.36.0 is vulnerable to an Arbitrary Memory Read vulnerability. The 0x22200B IOCTL code of the Vba32m64.sys driver allows to read up to 0x802 of memory from ar arbitrary user-supplied pointer.	2024-02-13	6.3	CVE-2024-23440
web-soudan -- mw_wp_form	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in websoudan MW WP Form allows Stored XSS.This issue affects MW WP Form: from n/a through 5.0.6.	2024-02-10	5.4	CVE-2024-24804
wolfssl -- sp_math_all_rsa	wolfSSL SP Math All RSA implementation is vulnerable to the Marvin Attack, new variation of a timing Bleichenbacher style attack, when built with the following options to configure: --enable-all CFLAGS="-DWOLFSSL_STATIC_RSA" The define "WOLFSSL_STATIC_RSA" enables static RSA cipher suites, which is not recommended, and has been disabled by default since wolfSSL 3.6.6. Therefore the default build since 3.6.6, even with "--enable-all", is not vulnerable to the Marvin Attack. The vulnerability is specific to static RSA cipher suites, and expected to be padding-independent. The vulnerability allows an attacker to decrypt ciphertexts and forge signatures after probing with a large number of test observations. However, the server's private key is not exposed.	2024-02-09	5.9	CVE-2023-6935
wolfssl -- sp_math_all_rsa	wolfSSL prior to 5.6.6 did not check that messages in one (D)TLS record do not span key boundaries. As a result, it was possible to combine (D)TLS messages using different keys into one (D)TLS record. The most extreme edge case is that, in (D)TLS 1.3, it was possible that an unencrypted (D)TLS 1.3 record from the server containing first a ServerHello message and then the rest of the first server flight would be accepted by a wolfSSL client. In (D)TLS 1.3 the handshake is encrypted after the ServerHello but a wolfSSL client would accept an unencrypted flight from the server. This does not compromise key negotiation and authentication so it is assigned a low severity rating.	2024-02-15	5.3	CVE-2023-6937
wordpress -- wordpress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in UnitedThemes Brooklyn | Creative Multi-Purpose Responsive WordPress Theme allows Reflected XSS. This issue affects Brooklyn | Creative Multi-Purpose Responsive WordPress Theme: from n/a through 4.9.7.6.	2024-02-12	6.1	CVE-2024-24927
wordpress -- wordpress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MyAgilePrivacy My Agile Privacy - The only GDPR solution for WordPress that you can truly trust allows Stored XSS. This issue affects My Agile Privacy - The only GDPR solution for WordPress that you can truly trust: from n/a through 2.1.7.	2024-02-10	5.4	CVE-2023-51404
wordpress -- wordpress	The Awesome Support - WordPress HelpDesk & Support Plugin plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the editor_html() function in all versions up to, and including, 6.1.7. This makes it possible for authenticated attackers, with subscriber-level access and above, to view password protected and draft posts.	2024-02-10	5.3	CVE-2024-0596
wordpress -- wordpress	The Event Manager, Events Calendar, Events Tickets for WooCommerce - Eventin plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the export_data() function in all versions up to, and including, 3.3.50. This makes it possible for unauthenticated attackers to export event data.	2024-02-09	5.3	CVE-2024-1122
wordpress -- wordpress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Start Booking Scheduling Plugin - Online Booking for WordPress allows Stored XSS.This issue affects Scheduling Plugin - Online Booking for WordPress: from n/a through 3.5.10.	2024-02-10	5.4	CVE-2024-23517
wordpress -- wordpress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Team Heateor Heateor Social Login WordPress allows Stored XSS. This issue affects Heateor Social Login WordPress: from n/a through 1.1.30.	2024-02-10	5.4	CVE-2024-24712

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Auto Listings Auto Listings - Car Listings & Car Dealership Plugin for WordPress allows Stored XSS. This issue affects Auto Listings - Car Listings & Car Dealership Plugin for WordPress: from n/a through 2.6.5.	2024-02-10	5.4	CVE-2024-24713
wordpress -- wordpress	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 4.8.0 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.	2024-02-13	6.4	CVE-2024-1159
wordpress -- wordpress	The Landing Page Cat - Coming Soon Page, Maintenance Page & Squeeze Pages plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.7.2. This makes it possible for unauthenticated attackers to access landing pages that may not be public.	2024-02-15	5.3	CVE-2024-0708
wordpress -- wordpress	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's button URL in all versions up to, and including, 4.8.0 due to insufficient input sanitization and output escaping. 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.	2024-02-13	5.4	CVE-2024-1157
wordpress -- wordpress	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Icon Link in all versions up to, and including, 4.8.0 due to insufficient input sanitization and output escaping. 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.	2024-02-13	5.4	CVE-2024-1160
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Contest Gallery Photos and Files Contest Gallery - Contact Form, Upload Form, Social Share and Voting Plugin for WordPress. This issue affects Photos and Files Contest Gallery - Contact Form, Upload Form, Social Share and Voting Plugin for WordPress: from n/a through 21.2.8.4.	2024-02-12	5.4	CVE-2024-24887
wp-hosting -- pay_with_vipps_and_mobilepay_for_woocommerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Hosting Pay with Vipps and MobilePay for WooCommerce allows Stored XSS.This issue affects Pay with Vipps and MobilePay for WooCommerce: from n/a through 1.14.13.	2024-02-10	5.4	CVE-2023-51485
wpoperation -- ultra_companion	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPoperation Ultra Companion - Companion plugin for WPoperation Themes allows Stored XSS.This issue affects Ultra Companion - Companion plugin for WPoperation Themes: from n/a through 1.1.9.	2024-02-10	5.4	CVE-2024-24803
wpsimpletools -- basic_log_viewer	Cross-Site Request Forgery (CSRF) vulnerability in WpSimpleTools Basic Log Viewer. This issue affects Basic Log Viewer: from n/a through 1.0.4.	2024-02-12	4.3	CVE-2024-24935
yannick_lefebvre -- link_library	Cross-Site Request Forgery (CSRF) vulnerability in Yannick Lefebvre Link Library. This issue affects Link Library: from n/a through 7.5.13.	2024-02-12	4.3	CVE-2024-24875
zabbix -- zabbix	The cause of vulnerability is improper validation of form input field "Name" on Graph page in Items section.	2024-02-09	5.4	CVE-2024-22119 security@zabbix.com
zalify -- easy_email	Cross Site Scripting (XSS) vulnerability in EasyEmail v.4.12.2 and before allows a local attacker to execute arbitrary code via the user input parameter(s). NOTE:	2024-02-09	6.1	CVE-2023-39683

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Researcher claims issue is present in all versions prior and later than tested version.			
zixn -- vk_poster_group	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Djo VK Poster Group allows Reflected XSS. This issue affects VK Poster Group: from n/a through 2.0.3.	2024-02-12	6.1	CVE-2024-24932
zoom_video_communications,_inc -- zoom_clients	Improper input validation in some Zoom clients may allow an authenticated user to conduct a denial of service via network access.	2024-02-14	5.4	CVE-2024-24690
zoom_video_communications_inc -- zoom_clients	Business logic error in some Zoom clients may allow an authenticated user to conduct information disclosure via network access.	2024-02-14	6.5	CVE-2024-24699
zoom_video_communications_inc -- zoom_clients	Improper authentication in some Zoom clients may allow a privileged user to conduct a disclosure of information via local access.	2024-02-14	4.9	CVE-2024-24698
zoom_video_communications_inc -- zoom_desktop_client_for_windows_zoom_vdi_client_for_windows_and_zoom_meeting_sdk_for_windows	Improper input validation in Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom Meeting SDK for Windows may allow an authenticated user to conduct a disclosure of information via network access.	2024-02-14	6.8	CVE-2024-24695
zoom_video_communications_inc -- zoom_desktop_client_for_windows_zoom_vdi_client_for_windows_and_zoom_meeting_sdk_for_windows	Improper input validation in Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom Meeting SDK for Windows may allow an authenticated user to conduct a disclosure of information via network access.	2024-02-14	6.8	CVE-2024-24696
1panel-dev -- 1panel	1Panel is an open source Linux server operation and maintenance management panel. The HTTPS cookie that comes with the panel does not have the Secure keyword, which may cause the cookie to be sent in plain text if accessed using HTTP. This issue has been patched in version 1.9.6.	2024-02-05	6.5	CVE-2024-24768
acowebs -- product_labels_for_woocommerce_(sale_badges)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Acowebs Product Labels For Woocommerce (Sale Badges) allows Stored XSS.This issue affects Product Labels For Woocommerce (Sale Badges): from n/a through 1.5.3.	2024-02-08	5.9	CVE-2024-24886
allegro_ai -- clearml	Allegro AI's open-source version of ClearML stores passwords in plaintext within the MongoDB instance, resulting in a compromised server leaking all user emails and passwords.	2024-02-05	6	CVE-2024-24595
ansible -- ansible	An information disclosure flaw was found in ansible-core due to a failure to respect the ANSIBLE_NO_LOG configuration in some scenarios. It was discovered that information is still included in the output in certain tasks, such as loop items. Depending on the task, this issue may include sensitive information, such as decrypted secret values.	2024-02-06	5	CVE-2024-0690

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
antisamy_project -- antisamy	AntiSamy is a library for performing fast, configurable cleansing of HTML coming from untrusted sources. Prior to 1.7.5, there is a potential for a mutation XSS (mXSS) vulnerability in AntiSamy caused by flawed parsing of the HTML being sanitized. To be subject to this vulnerability the `preserveComments` directive must be enabled in your policy file. As a result, certain crafty inputs can result in elements in comment tags being interpreted as executable when using AntiSamy's sanitized output. Patched in AntiSamy 1.7.5 and later.	2024-02-02	6.1	CVE-2024-23635
apache_software_foundation -- ozone	Improper Authentication vulnerability in Apache Ozone. The vulnerability allows an attacker to download metadata internal to the Storage Container Manager service without proper authentication. The attacker is not allowed to do any modification within the Ozone Storage Container Manager service using this vulnerability. The accessible metadata does not contain sensitive information that can be used to exploit the system later on, and the accessible data does not make it possible to gain access to actual user data within Ozone. This issue affects Apache Ozone: 1.2.0 and subsequent releases up until 1.3.0. Users are recommended to upgrade to version 1.4.0, which fixes the issue.	2024-02-07	5.3	CVE-2023-39196
apollo13themes -- apollo13_framework_extensions	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Apollo13Themes Apollo13 Framework Extensions allows Stored XSS. This issue affects Apollo13 Framework Extensions: from n/a through 1.9.2.	2024-02-08	6.5	CVE-2024-24880
audrasjb -- gdpr_data_request_form	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Audrasjb GDPR Data Request Form allows Stored XSS. This issue affects GDPR Data Request Form: from n/a through 1.6.	2024-02-08	6.5	CVE-2024-24836
axis_communications_ab -- axis_os	Brandon Rothel from QED Secure Solutions has found that the VAPIX API tcptest.cgi did not have a sufficient input validation allowing for a possible remote code execution. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service account. The impact of exploiting this vulnerability is lower with operator-privileges compared to administrator-privileges service accounts. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution.	2024-02-05	6.3	CVE-2023-5677
axis_communications_ab -- axis_os	Vintage, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API create_overlay.cgi did not have a sufficient input validation allowing for a possible remote code execution. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service account. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution.	2024-02-05	5.4	CVE-2023-5800
beijing_baichuo -- smart_s20_management_platform	A vulnerability, which was classified as critical, was found in Beijing Baichuo Smart S20 Management Platform up to 20231120. This affects an unknown part of the file /sysmanage/sysmanageajax.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-252993 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-06	4.7	CVE-2024-1254
beijing_baichuo -- smart_s40_management_platform	A vulnerability, which was classified as critical, has been found in Beijing Baichuo Smart S40 Management Platform up to 20240126. Affected by this issue is some unknown functionality of the file /useratte/web.php of the component Import Handler. The manipulation of the argument file_upload 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-252992. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-06	4.7	CVE-2024-1253
blockmason -- credit-protocol	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in blockmason credit-protocol. It has been declared as problematic. Affected by this vulnerability	2024-02-04	4.3	CVE-2018-25098

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	is the function executeUcacTx of the file contracts/CreditProtocol.sol of the component UCAC Handler. The manipulation leads to denial of service. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The patch is named 082e01f18707ef995e80ebe97fcedb229a55efc5. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-252799. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.			
blurams -- lumi_security_camera_a31c_firmware	An issue in Blurams Lumi Security Camera (A31C) v.2.3.38.12558 allows a physically proximate attackers to execute arbitrary code.	2024-02-02	6.8	CVE-2023-51820
br-automation -- automation_runtime	A reflected cross-site scripting (XSS) vulnerability exists in the SVG version of System Diagnostics Manager of B&R Automation Runtime versions <= G4.93 that enables a remote attacker to execute arbitrary JavaScript code in the context of the attacked user's browser session.	2024-02-05	6.1	CVE-2023-6028
ckeditor -- ckeditor4	CKEditor4 is an open source what-you-see-is-what-you-get HTML editor. A cross-site scripting vulnerability has been discovered in the core HTML parsing module in versions of CKEditor4 prior to 4.24.0-lts. It may affect all editor instances that enabled full-page editing mode or enabled CDATA elements in Advanced Content Filtering configuration (defaults to `script` and `style` elements). The vulnerability allows attackers to inject malformed HTML content bypassing Advanced Content Filtering mechanism, which could result in executing JavaScript code. An attacker could abuse faulty CDATA content detection and use it to prepare an intentional attack on the editor. A fix is available in version 4.24.0-lts.	2024-02-07	6.1	CVE-2024-24815
ckeditor -- ckeditor4	CKEditor4 is an open source what-you-see-is-what-you-get HTML editor. A cross-site scripting vulnerability vulnerability has been discovered in versions prior to 4.24.0-lts in samples that use the `preview` feature. All integrators that use these samples in the production code can be affected. The vulnerability allows an attacker to execute JavaScript code by abusing the misconfigured preview feature. It affects all users using the CKEditor 4 at version < 4.24.0-lts with affected samples used in a production environment. A fix is available in version 4.24.0-lts.	2024-02-07	6.1	CVE-2024-24816
clicktotweet.com -- click_to_tweet	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ClickToTweet.Com Click To Tweet allows Stored XSS.This issue affects Click To Tweet: from n/a through 2.0.14.	2024-02-10	6.5	CVE-2024-23514
codeastro -- employee_task_management_system	A vulnerability has been found in CodeAstro Employee Task Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file \employee-tasks-php\attendance-info.php. The manipulation of the argument aten_id 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-252697 was assigned to this vulnerability.	2024-02-03	5.4	CVE-2024-1199
codeastro -- restaurant_pos_system	A vulnerability, which was classified as critical, was found in CodeAstro Restaurant POS System 1.0. This affects an unknown part of the file update_product.php. The manipulation leads to unrestricted upload. 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-253011.	2024-02-07	6.3	CVE-2024-1268
creative_themes -- blocksy	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Creative Themes Blocksy allows Stored XSS. This issue affects Blocksy: from n/a through 2.0.19.	2024-02-08	6.5	CVE-2024-24871
cryptlib -- cryptlib	A security vulnerability has been identified in the cryptlib cryptographic library when cryptlib is compiled with the support for RSA key exchange ciphersuites in TLS (by setting the USE_RSA_SUITES define), it will be vulnerable to the timing variant of the Bleichenbacher attack. An attacker that is able to perform a large	2024-02-05	5.9	CVE-2024-0202

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	number of connections to the server will be able to decrypt RSA ciphertexts or forge signatures using server's certificate.			
cups_easy -- 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/locationcreate.php, in the locationid 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.	2024-02-02	6.1	CVE-2024-23895
dan_dulaney -- dan's_embedder_for_google_calendar	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dan Dulaney Dan's Embedder for Google Calendar allows Stored XSS. This issue affects Dan's Embedder for Google Calendar: from n/a through 1.2.	2024-02-05	6.5	CVE-2023-51504
dell -- appsync	Dell EMC AppSync, versions from 4.2.0.0 to 4.6.0.0 including all Service Pack releases, contain an exposure of sensitive information vulnerability in AppSync server logs. A high privileged remote attacker could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable system with privileges of the compromised account.	2024-02-08	6.2	CVE-2024-22464
dell -- cpg_bios	Dell BIOS contains a Signed to Unsigned Conversion Error vulnerability. A local authenticated malicious user with admin privileges could potentially exploit this vulnerability, leading to denial of service.	2024-02-06	6.7	CVE-2023-28063
dell -- dell_bsafe_ssl-j	Dell BSAFE SSL-J, versions prior to 6.5, and versions 7.0 and 7.1 contain a debug message revealing unnecessary information vulnerability. This may lead to disclosing sensitive information to a locally privileged user.	2024-02-10	4.4	CVE-2023-28077
dell -- dell_command_monitor	Dell Command | Monitor, versions prior to 10.9, contain an arbitrary folder deletion vulnerability. A locally authenticated malicious user may exploit this vulnerability in order to perform a privileged arbitrary file delete.	2024-02-06	4.7	CVE-2023-28049
dell -- dell_display_manager	Dell Display Manager application, version 2.1.1.17 and prior, contain an insecure operation on windows junction/mount point. A local malicious user could potentially exploit this vulnerability during installation leading to arbitrary folder or file deletion	2024-02-06	6.6	CVE-2023-32474
dell -- dell_encryption	Dell Encryption, Dell Endpoint Security Suite Enterprise, and Dell Security Management Server versions prior to 11.9.0 contain privilege escalation vulnerability due to improper ACL of the non-default installation directory. A local malicious user could potentially exploit this vulnerability by replacing binaries in installed directory and taking reverse shell of the system leading to Privilege Escalation.	2024-02-06	6.7	CVE-2023-32479
dell -- dup_framework	DUP framework version 4.9.4.36 and prior contains insecure operation on Windows junction/Mount point vulnerability. A local malicious standard user could exploit the vulnerability to create arbitrary files, leading to denial of service	2024-02-06	6.3	CVE-2023-32454
dev.dans-art -- add_customer_for_woocommerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dan's Art Add Customer for WooCommerce allows Stored XSS.This issue affects Add Customer for WooCommerce: from n/a through 1.7.	2024-02-05	4.8	CVE-2024-24841
elastic -- apm_server	An issue was discovered whereby APM Server could log at ERROR level, a response from Elasticsearch indicating that indexing the document failed and that response would contain parts of the original document. Depending on the nature of the document that the APM Server attempted to ingest, this could lead to the insertion of sensitive or private information in the APM Server logs.	2024-02-07	5.7	CVE-2024-23448

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
elastic -- elastic_network_drive_connector	An issue was discovered in the Windows Network Drive Connector when using Document Level Security to assign permissions to a file, with explicit allow write and deny read. Although the document is not accessible to the user in Network Drive it is visible in search applications to the user.	2024-02-07	5.3	CVE-2024-23447
elastic -- kibana	An issue was discovered by Elastic, whereby the Detection Engine Search API does not respect Document-level security (DLS) or Field-level security (FLS) when querying the .alerts-security.alerts-{space_id} indices. Users who are authorized to call this API may obtain unauthorized access to documents if their roles are configured with DLS or FLS against the aforementioned index.	2024-02-07	6.5	CVE-2024-23446
emerson -- rosemount_gc370xa	In Emerson Rosemount GC370XA, GC700XA, and GC1500XA products, an unauthenticated user with network access could obtain access to sensitive information or cause a denial-of-service condition.	2024-02-09	6.9	CVE-2023-43609
emerson -- rosemount_gc370xa	In Emerson Rosemount GC370XA, GC700XA, and GC1500XA products, an authenticated user with network access could run arbitrary commands from a remote computer.	2024-02-09	6.9	CVE-2023-49716
enalean -- tuleap	Tuleap is an Open Source Suite to improve management of software developments and collaboration. Some users might get access to restricted information when a process validates the permissions of multiple users (e.g. mail notifications). This issue has been patched in version 15.4.99.140 of Tuleap Community Edition.	2024-02-06	5.3	CVE-2024-23344
envoyproxy -- envoy	Envoy is a high-performance edge/middle/service proxy. The regex expression is compiled for every request and can result in high CPU usage and increased request latency when multiple routes are configured with such matchers. This issue has been addressed in released 1.29.1, 1.28.1, 1.27.3, and 1.26.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-09	4.3	CVE-2024-23323
fivestarplugins -- five_star_restaurant_menu	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Five Star Plugins Five Star Restaurant Reviews allows Stored XSS.This issue affects Five Star Restaurant Reviews: from n/a through 2.3.5.	2024-02-05	5.4	CVE-2024-24838
forum_one -- wp-cfm	Cross-Site Request Forgery (CSRF) vulnerability in Forum One WP-CFM wp-cfm. This issue affects WP-CFM: from n/a through 1.7.8.	2024-02-07	5.4	CVE-2024-24706
frappe -- frappe	Frappe is a full-stack web application framework that uses Python and MariaDB on the server side and a tightly integrated client side library. Prior to versions 14.59.0 and 15.5.0, portal pages are susceptible to Cross-Site Scripting (XSS) which can be used to inject malicious JS code if user clicks on a malicious link. This vulnerability has been patched in versions 14.59.0 and 15.5.0. No known workarounds are available.	2024-02-07	5.4	CVE-2024-24812
galleon -- eap_eap-xp_servers	An improper initialization vulnerability was found in Galleon. When using Galleon to provision custom EAP or EAP-XP servers, the servers are created unsecured. This issue could allow an attacker to access remote HTTP services available from the server.	2024-02-06	6.8	CVE-2023-4503
getsentry -- sentry	Sentry is an error tracking and performance monitoring platform. Sentry's integration platform provides a way for external services to interact with Sentry. One of such integrations, the Phabricator integration (maintained by Sentry) with version <=24.1.1 contains a constrained SSRF vulnerability. An attacker could make Sentry send POST HTTP requests to arbitrary URLs (including internal IP addresses) by providing an unsanitized input to the Phabricator integration. However, the body payload is constrained to a specific format. If an attacker has access to a Sentry instance, this allows them to: 1. interact with internal network; 2. scan local/remote ports. This issue has been fixed in Sentry self-hosted release 24.1.2, and has already been mitigated on sentry.io on February 8. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-09	4.3	CVE-2024-24829

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gitlab -- gitlab	An issue has been discovered in GitLab EE Premium and Ultimate affecting versions 16.4.3, 16.5.3, and 16.6.1. In projects using subgroups to define who can push and/or merge to protected branches, there may have been instances in which subgroup members with the Developer role were able to push or merge to protected branches.	2024-02-08	6.5	CVE-2023-6564
gitlab -- gitlab	An issue has been discovered in GitLab EE affecting all versions starting from 11.3 before 16.6.7, all versions starting from 16.7 before 16.7.5, all versions starting from 16.8 before 16.8.2. It was possible for an attacker to cause a client-side denial of service using malicious crafted content in the CODEOWNERS file.	2024-02-07	6.5	CVE-2023-6736
gitlab -- gitlab	An issue has been discovered in GitLab EE affecting all versions from 16.4 prior to 16.6.7, 16.7 prior to 16.7.5, and 16.8 prior to 16.8.2 which allows a maintainer to change the name of a protected branch that bypasses the security policy added to block MR.	2024-02-07	6.7	CVE-2023-6840
gitlab -- gitlab	An issue has been discovered in GitLab EE affecting all versions from 13.3.0 prior to 16.6.7, 16.7 prior to 16.7.5, and 16.8 prior to 16.8.2 which allows an attacker to do a resource exhaustion using GraphQL `vulnerabilitiesCountByDay`	2024-02-07	6.5	CVE-2024-1066
globalscape -- cuteftp	A vulnerability was found in Global Scape CuteFTP 9.3.0.3 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument Host/Username/Password leads to denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252680. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-02	5.5	CVE-2024-1190
gnu -- coreutils	A flaw was found in the GNU coreutils "split" program. A heap overflow with user-controlled data of multiple hundred bytes in length could occur in the line_bytes_split() function, potentially leading to an application crash and denial of service.	2024-02-06	5.5	CVE-2024-0684
google -- android	In TVAPI, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03961601; Issue ID: DTV03961601.	2024-02-05	6.7	CVE-2024-20001
google -- android	In TVAPI, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03961715; Issue ID: DTV03961715.	2024-02-05	6.7	CVE-2024-20002
google -- android	In keyInstall, there is a possible escalation of privilege due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08358560; Issue ID: ALPS08358560.	2024-02-05	6.7	CVE-2024-20010
google -- android	In keyInstall, there is a possible escalation of privilege due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08358566; Issue ID: ALPS08358566.	2024-02-05	6.7	CVE-2024-20012
google -- android	In keyInstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08471742; Issue ID: ALPS08308608.	2024-02-05	6.7	CVE-2024-20013
google -- android	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation Patch ID: ALPS07835901; Issue ID: ALPS07835901.	2024-02-05	4.4	CVE-2024-20016

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
graylog -- graylog	Graylog is a free and open log management platform. Starting in version 4.3.0 and prior to versions 5.1.11 and 5.2.4, reauthenticating with an existing session cookie would re-use that session id, even if for different user credentials. In this case, the pre-existing session could be used to gain elevated access to an existing Graylog login session, provided the malicious user could successfully inject their session cookie into someone else's browser. The complexity of such an attack is high, because it requires presenting a spoofed login screen and injection of a session cookie into an existing browser, potentially through a cross-site scripting attack. No such attack has been discovered. Graylog 5.1.11 and 5.2.4, and any versions of the 6.0 development branch, contain patches to not re-use sessions under any circumstances. Some workarounds are available. Using short session expiration and explicit log outs of unused sessions can help limiting the attack vector. Unpatched this vulnerability exists, but is relatively hard to exploit. A proxy could be leveraged to clear the `authentication` cookie for the Graylog server URL for the `/api/system/sessions` endpoint, as that is the only one vulnerable.	2024-02-07	5.7	CVE-2024-24823
hcl -- bigfix	A cross-site scripting (XSS) vulnerability in the Web Reports component of HCL BigFix Platform can possibly allow an attack to exploit an application parameter during execution of the Save Report.	2024-02-03	6.5	CVE-2023-37528
hcl-- devops_deploy	HCL DevOps Deploy / HCL Launch (UCD) could disclose sensitive user information when installing the Windows agent.	2024-02-03	6.2	CVE-2024-23550
hcl_software -- hcl_sametime	Sametime is impacted by a Cross Site Request Forgery (CSRF) vulnerability. Some REST APIs in the Sametime Proxy application can allow an attacker to perform malicious actions on the application.	2024-02-09	5.9	CVE-2023-50349
hcl_software -- hcl_sametime	Sametime is impacted by sensitive fields with autocomplete enabled in the Legacy web chat client. By default, this allows user entered data to be stored by the browser.	2024-02-10	4	CVE-2023-45696
hcl_software -- hcl_sametime	Sametime is impacted by lack of clickjacking protection in Outlook add-in. The application is not implementing appropriate protections in order to protect users from clickjacking attacks.	2024-02-10	4.8	CVE-2023-45698
hcltech -- bigfix_platform	A reflected cross-site scripting (XSS) vulnerability in the Web Reports component of HCL BigFix Platform can possibly allow an attacker to execute malicious javascript code in the application session or in database, via remote injection, while rendering content in a web page.	2024-02-02	6.1	CVE-2023-37527
hcltech -- bigfix_platform	A cross-site scripting (XSS) vulnerability in the Web Reports component of HCL BigFix Platform exists due to missing a specific http header attribute.	2024-02-02	5.4	CVE-2024-23553
hid_global -- hid_iclass_se_reader_configuration_cards	Sensitive data can be extracted from HID iCLASS SE reader configuration cards. This could include credential and device administrator keys.	2024-02-07	5.3	CVE-2024-23806
hid_global -- iclass_se_cp1000_encoder	Certain configuration available in the communication channel for encoders could expose sensitive data when reader configuration cards are programmed. This data could include credential and device administration keys.	2024-02-06	5.9	CVE-2024-22388
howard_ehrenberg -- custom_post_carousels_with_owl	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Howard Ehrenberg Custom Post Carousels with Owl allows Stored XSS. This issue affects Custom Post Carousels with Owl: from n/a through 1.4.6.	2024-02-10	6.5	CVE-2023-51493
ibm -- aspera_faspex	IBM Aspera Faspex 5.0.6 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 236441.	2024-02-02	5.4	CVE-2022-40744

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- business_automation_workflow	IBM Business Automation Workflow 22.0.2, 23.0.1, and 23.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 275665.	2024-02-04	5.4	CVE-2023-50947
ibm -- engineering_lifecycle_optimization_publishing	IBM Engineering Lifecycle Optimization - Publishing 7.0.2 and 7.0.3 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 268749.	2024-02-09	6.3	CVE-2023-45187
ibm -- engineering_lifecycle_optimization_publishing	IBM Engineering Lifecycle Optimization 7.0.2 and 7.0.3 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: 268754.	2024-02-09	5.1	CVE-2023-45190
ibm -- i_access_client_solutions	IBM i Access Client Solutions (ACS) 1.1.2 through 1.1.4 and 1.1.4.3 through 1.1.9.4 is vulnerable to NT LAN Manager (NTLM) hash disclosure by an attacker modifying UNC capable paths within ACS configuration files to point to a hostile server. If NTLM is enabled, the Windows operating system will try to authenticate using the current user's session. The hostile server could capture the NTLM hash information to obtain the user's credentials. IBM X-Force ID: 279091.	2024-02-09	5.1	CVE-2024-22318
ibm -- integration_bus_for_z/os	The IBM Integration Bus for z/OS 10.1 through 10.1.0.2 AdminAPI is vulnerable to a denial of service due to file system exhaustion. IBM X-Force ID: 279972.	2024-02-09	6.5	CVE-2024-22332
ibm -- powersc	IBM PowerSC 1.3, 2.0, and 2.1 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. IBM X-Force ID: 275113.	2024-02-02	6.1	CVE-2023-50933
ibm -- powersc	IBM PowerSC 1.3, 2.0, and 2.1 fails to properly restrict access to a URL or resource, which may allow a remote attacker to obtain unauthorized access to application functionality and/or resources. IBM X-Force ID: 275115.	2024-02-02	6.5	CVE-2023-50935
ibm -- powersc	IBM PowerSC 1.3, 2.0, and 2.1 uses insecure HTTP methods which could allow a remote attacker to perform unauthorized file request modification. IBM X-Force ID: 275109.	2024-02-02	5.3	CVE-2023-50327
ibm -- powersc	IBM PowerSC 1.3, 2.0, and 2.1 may allow a remote attacker to view session identifiers passed via URL query strings. IBM X-Force ID: 275110.	2024-02-02	5.3	CVE-2023-50328
ibm -- powersc	IBM PowerSC 1.3, 2.0, and 2.1 uses single-factor authentication which can lead to unnecessary risk of compromise when compared with the benefits of a dual-factor authentication scheme. IBM X-Force ID: 275114.	2024-02-02	5.3	CVE-2023-50934
ibm -- powersc	IBM PowerSC 1.3, 2.0, and 2.1 does not provide logout functionality, which could allow an authenticated user to gain access to an unauthorized user using session fixation. IBM X-Force ID: 275131.	2024-02-02	5.4	CVE-2023-50941
ibm -- powersc	IBM PowerSC 1.3, 2.0, and 2.1 MFA does not implement the "HTTP Strict Transport Security" (HSTS) web security policy mechanism. IBM X-Force ID: 276004.	2024-02-02	5.9	CVE-2023-50962
ibm -- powersc	IBM PowerSC 1.3, 2.0, and 2.1 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 275128.	2024-02-02	4.3	CVE-2023-50938
ibm -- powervm_hypervisor	IBM PowerVM Hypervisor FW950.00 through FW950.90, FW1020.00 through FW1020.40, and FW1030.00 through FW1030.30 could allow a system administrator to obtain sensitive partition information. IBM X-Force ID: 269695.	2024-02-06	5.3	CVE-2023-46183

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_access_manager_container	IBM Security Access Manager Container 10.0.0.0 through 10.0.6.1 temporarily stores sensitive information in files that could be accessed by a local user. IBM X-Force ID: 254657.	2024-02-07	5.5	CVE-2023-31002
ibm -- security_verify_access_appliance/security_verify_access_docker	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 10.0.0.0 through 10.0.6.1) could allow a user to download files from an incorrect repository due to improper file validation. IBM X-Force ID: 254972.	2024-02-03	5.5	CVE-2023-32329
ibm -- semeru_runtime	IBM Semeru Runtime 8.0.302.0 through 8.0.392.0, 11.0.12.0 through 11.0.21.0, 17.0.1.0 - 17.0.9.0, and 21.0.1.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 281222.	2024-02-10	5.9	CVE-2024-22361
ibm -- soar_qradar_plugin_app	IBM SOAR QRadar Plugin App 1.0 through 5.0.3 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: 260575.	2024-02-02	6.5	CVE-2023-38019
ibm -- soar_qradar_plugin_app	IBM SOAR QRadar Plugin App 1.0 through 5.0.3 could allow an authenticated user to manipulate output written to log files. IBM X-Force ID: 260576.	2024-02-02	4.3	CVE-2023-38020
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator 6.0.0.0 through 6.0.3.8 and 6.1.0.0 through 6.1.2.3 could allow an authenticated user to cause a denial of service due to uncontrolled resource consumption. IBM X-Force ID: 255827.	2024-02-09	6.5	CVE-2023-32341
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.8 and 6.1.0.0 through 6.1.2.3 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 265559.	2024-02-09	4.3	CVE-2023-42016
ibm -- storage_ceph	IBM Storage Ceph 5.3z1, 5.3z5, and 6.1z1 could allow an authenticated user on the network to cause a denial of service from RGW. IBM X-Force ID: 268906.	2024-02-02	6.5	CVE-2023-46159
ibm -- storage_defender-resiliency_service	IBM Storage Defender - Resiliency Service 2.0 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 278748.	2024-02-10	4.4	CVE-2024-22312
ibm -- storage_defender_resiliency_service	IBM Storage Defender - Resiliency Service 2.0 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: 278749.	2024-02-10	6.2	CVE-2024-22313
ibm -- storage_virtualize	IBM SAN Volume Controller, IBM Storwize, IBM FlashSystem and IBM Storage Virtualize 8.6 products could allow a remote attacker to spoof a trusted system that would not be correctly validated by the Storwize server. This could lead to a user connecting to a malicious host, believing that it was a trusted system and deceived into accepting spoofed data. IBM X-Force ID: 271016.	2024-02-07	5.9	CVE-2023-47700
ibm -- tivoli_application_dependency_discovery_manager	IBM Tivoli Application Dependency Discovery Manager 7.3.0.0 through 7.3.0.10 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 270271.	2024-02-02	6.1	CVE-2023-47144
ibm -- urbancode_deploy	IBM UrbanCode Deploy (UCD) 7.0 through 7.0.5.19, 7.1 through 7.1.2.15, 7.2 through 7.2.3.8, 7.3 through 7.3.2.3, and IBM UrbanCode Deploy (UCD) - IBM DevOps Deploy 8.0.0.0 could disclose sensitive user information when installing the Windows agent. IBM X-Force ID: 279971.	2024-02-06	6.2	CVE-2024-22331

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm--powervm_hypervisor	IBM PowerVM Hypervisor FW950.00 through FW950.90, FW1020.00 through FW1020.40, and FW1030.00 through FW1030.30 could reveal sensitive partition data to a system administrator. IBM X-Force ID: 257135.	2024-02-04	5.3	CVE-2023-33851
icinga -- icingaweb2-module-incubator	icingaweb2-module-incubator is a working project of bleeding edge Icinga Web 2 libraries. In affected versions the class `gipfl\Web\Form` is the base for various concrete form implementations [1] and provides protection against cross site request forgery (CSRF) by default. This is done by automatically adding an element with a CSRF token to any form, unless explicitly disabled, but even if enabled, the CSRF token (sent during a client's submission of a form relying on it) is not validated. This enables attackers to perform changes on behalf of a user which, unknowingly, interacts with a prepared link or website. The version 0.22.0 is available to remedy this issue. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-09	5.3	CVE-2024-24819
if_so_plugin -- if-so_dynamic_content_personalization	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in If So Plugin If-So Dynamic Content Personalization allows Stored XSS. This issue affects If-So Dynamic Content Personalization: from n/a through 1.6.3.1.	2024-02-10	6.5	CVE-2023-51492
indent--indent_2.2.13	A flaw was found in Indent. This issue may allow a local user to use a specially-crafted file to trigger a heap-based buffer overflow, which can lead to an application crash.	2024-02-06	5.5	CVE-2024-0911
itop -- vpn	A vulnerability classified as critical was found in iTop VPN up to 4.0.0.1. Affected by this vulnerability is an unknown functionality in the library ITopVpnCallbackProcess.sys of the component IOCTL Handler. The manipulation leads to denial of service. The attack needs to be approached locally. The identifier VDB-252685 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-02	5.5	CVE-2024-1195
jetbrains -- intellij_idea	In JetBrains IntelliJ IDEA before 2023.3.3 a plugin for JetBrains Space was able to send an authentication token to an inappropriate URL	2024-02-06	5.3	CVE-2024-24941
jetbrains -- intellij_idea	In JetBrains IntelliJ IDEA before 2023.3.3 path traversal was possible when unpacking archives	2024-02-06	4.3	CVE-2024-24940
jetbrains -- rider	In JetBrains Rider before 2023.3.3 logging of environment variables containing secret values was possible	2024-02-06	5.3	CVE-2024-24939
jetbrains -- teamcity	In JetBrains TeamCity before 2023.11.2 access control at the S3 Artifact Storage plugin endpoint was missed	2024-02-06	5.3	CVE-2024-24936
jetbrains -- teamcity	In JetBrains TeamCity before 2023.11.2 stored XSS via agent distribution was possible	2024-02-06	5.4	CVE-2024-24937
jetbrains -- teamcity	In JetBrains TeamCity before 2023.11.2 limited directory traversal was possible in the Kotlin DSL documentation	2024-02-06	5.3	CVE-2024-24938
jetbrains -- teamcity	In JetBrains TeamCity before 2023.11.3 path traversal allowed reading data within JAR archives	2024-02-06	5.3	CVE-2024-24942
jetbrains -- toolbox	In JetBrains Toolbox App before 2.2 a DoS attack was possible via a malicious SVG image	2024-02-06	5.5	CVE-2024-24943
jgadbois -- calculatorpro_calculators	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jgadbois CalculatorPro Calculators allows Reflected XSS.This issue affects CalculatorPro Calculators: from n/a through 1.1.7.	2024-02-05	6.1	CVE-2024-24847
jspxcms -- jspxcms	A vulnerability was found in Jspxcms 10.2.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /template/1/default/. The manipulation leads to information disclosure. The attack may be launched	2024-02-03	5.3	CVE-2024-1200

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remotely. Theexploit has been disclosed to the public and may be used. VDB-252698 is the identifier assigned to this vulnerability.			
juanpao -- jpshop	A vulnerability was found in Juanpao JPShop up to 1.5.02. It has been rated as critical. Affected by this issue is some unknown functionality of the file /api/controllers/admin/app/AppController.php of the component API. The manipulation of the argument app_pic_url leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-252998 is the identifier assigned to this vulnerability.	2024-02-06	6.3	CVE-2024-1259
juanpao -- jpshop	A vulnerability classified as critical has been found in Juanpao JPShop up to 1.5.02. This affects the function actionIndex of the file /api/controllers/admin/app/ComboController.php of the component API. The manipulation of the argument pic_url leads to unrestricted upload. 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-252999.	2024-02-06	6.3	CVE-2024-1260
juanpao -- jpshop	A vulnerability classified as critical was found in Juanpao JPShop up to 1.5.02. This vulnerability affects the function actionIndex of the file /api/controllers/merchant/app/ComboController.php of the component API. The manipulation of the argument pic_url 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-253000.	2024-02-06	6.3	CVE-2024-1261
juanpao -- jpshop	A vulnerability, which was classified as critical, has been found in Juanpao JPShop up to 1.5.02. This issue affects the function actionUpdate of the file /api/controllers/merchant/design/MaterialController.php of the component API. The manipulation of the argument pic_url leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-253001 was assigned to this vulnerability.	2024-02-06	6.3	CVE-2024-1262
juanpao -- jpshop	A vulnerability, which was classified as critical, was found in Juanpao JPShop up to 1.5.02. Affected is the function actionUpdate of the file /api/controllers/merchant/shop/PosterController.php of the component API. The manipulation of the argument pic_url leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-253002 is the identifier assigned to this vulnerability.	2024-02-06	6.3	CVE-2024-1263
juanpao -- jpshop	A vulnerability has been found in Juanpao JPShop up to 1.5.02 and classified as critical. Affected by this vulnerability is the function actionUpdate of the file /api/controllers/common/UploadsController.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 associated identifier of this vulnerability is VDB-253003.	2024-02-07	6.3	CVE-2024-1264
leanote -- leanote	Leanote version 2.7.0 allows obtaining arbitrary local files. This is possible because the application is vulnerable to LFR.	2024-02-07	5.5	CVE-2024-0849
leap13 -- premium_addons_for_elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Leap13 Premium Addons for Elementor allows Stored XSS. This issue affects Premium Addons for Elementor: from n/a through 4.10.16.	2024-02-10	6.5	CVE-2024-24831
libexpat_project -- libexpat	libexpat through 2.5.0 allows recursive XML Entity Expansion if XML_DTD is undefined at compile time.	2024-02-04	5.5	CVE-2023-52426
liferay -- portal/dxp	The Document and Media widget In Liferay Portal 7.2.0 through 7.3.6, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 13, and older unsupported versions, does not limit resource consumption when generating a preview image, which allows remote authenticated users to cause a denial of service (memory consumption) via crafted PNG images.	2024-02-07	6.5	CVE-2024-25143

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
liferay -- portal/dxp	Account lockout in Liferay Portal 7.2.0 through 7.3.0, and older unsupported versions, and Liferay DXP 7.2 before fix pack 5, and older unsupported versions does not invalidate existing user sessions, which allows remote authenticated users to remain authenticated after an account has been locked.	2024-02-08	5.4	CVE-2023-47798
liferay -- portal/dxp	Liferay Portal 7.2.0 through 7.4.1, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 18, and older unsupported versions returns with different responses depending on whether a site does not exist or if the user does not have permission to access the site, which allows remote attackers to discover the existence of sites by enumerating URLs. This vulnerability occurs if locale.prepend.friendly.url.style=2 and if a custom 404 page is used.	2024-02-08	5.3	CVE-2024-25146
liferay -- portal/dxp	In Liferay Portal 7.2.0 through 7.4.1, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 15, and older unsupported versions the `doAsUserId` URL parameter may get leaked when creating linked content using the WYSIWYG editor and while impersonating a user. This may allow remote authenticated users to impersonate a user after accessing the linked content.	2024-02-08	5.4	CVE-2024-25148
liferay -- portal/dxp	The IFrame widget in Liferay Portal 7.2.0 through 7.4.3.26, and older unsupported versions, and Liferay DXP 7.4 before update 27, 7.3 before update 6, 7.2 before fix pack 19, and older unsupported versions does not check the URL of the IFrame, which allows remote authenticated users to cause a denial-of-service (DoS) via a self referencing IFrame.	2024-02-08	4.1	CVE-2024-25144
linecorp -- central_dogma	Central Dogma versions prior to 0.64.1 is vulnerable to Cross-Site Scripting (XSS), which could allow for the leakage of user sessions and subsequent authentication bypass.	2024-02-02	6.1	CVE-2024-1143
linksys -- wrt54gl	A vulnerability was found in Linksys WRT54GL 4.30.18 and classified as problematic. Affected by this issue is some unknown functionality of the file /SysInfo.htm of the component Web Management Interface. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-253328. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-09	4.3	CVE-2024-1404
linksys -- wrt54gl	A vulnerability was found in Linksys WRT54GL 4.30.18. It has been classified as problematic. This affects an unknown part of the file /wlaninfo.htm of the component Web Management Interface. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. The identifier VDB-253329 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-10	4.3	CVE-2024-1405
linksys -- wrt54gl	A vulnerability was found in Linksys WRT54GL 4.30.18. It has been declared as problematic. This vulnerability affects unknown code of the file /SysInfo1.htm of the component Web Management Interface. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. VDB-253330 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-10	4.3	CVE-2024-1406
linux -- kernel	A Marvin vulnerability side-channel leakage was found in the RSA decryption operation in the Linux Kernel. This issue may allow a network attacker to decrypt ciphertexts or forge signatures, limiting the services that use that private key.	2024-02-04	6.5	CVE-2023-6240
linux -- kernel	A flaw was found in the Linux kernel's NVMe driver. This issue may allow an unauthenticated malicious actor to send a set of crafted TCP packages when using NVMe over TCP, leading the NVMe driver to a NULL pointer dereference in the NVMe driver and causing kernel panic and a denial of service.	2024-02-07	6.5	CVE-2023-6356
linux -- kernel	A flaw was found in the Linux kernel's NVMe driver. This issue may allow an unauthenticated malicious actor to send a set of crafted TCP packages when using	2024-02-07	6.5	CVE-2023-6535

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	NVMe over TCP, leading the NVMe driver to a NULL pointer dereference in the NVMe driver, causing kernel panic and a denial of service.			
linux -- kernel	A flaw was found in the Linux kernel's NVMe driver. This issue may allow an unauthenticated malicious actor to send a set of crafted TCP packages when using NVMe over TCP, leading the NVMe driver to a NULL pointer dereference in the NVMe driver, causing kernel panic and a denial of service.	2024-02-07	6.5	CVE-2023-6536
linux -- kernel	A race condition was found in the Linux kernel's net/bluetooth device driver in conn_info_{min,max}_age_set() function. This can result in integrity overflow issue, possibly leading to bluetooth connection abnormality or denial of service.	2024-02-05	6.8	CVE-2024-24857
linux -- kernel	A race condition was found in the Linux kernel's media/xc4000 device driver in xc4000 xc4000_get_frequency() function. This can result in return value overflow issue, possibly leading to malfunction or denial of service issue.	2024-02-05	6.3	CVE-2024-24861
linux -- kernel	A use-after-free flaw was found in the Linux kernel's Memory Management subsystem when a user wins two races at the same time with a fail in the mas_prev_slot function. This issue could allow a local user to crash the system.	2024-02-08	5.1	CVE-2024-1312
linux -- kernel	A race condition was found in the Linux kernel's net/bluetooth in {conn,adv}_{min,max}_interval_set() function. This can result in l2cap connection or broadcast abnormality issue, possibly leading to denial of service.	2024-02-05	5.3	CVE-2024-24858
linux -- kernel	A race condition was found in the Linux kernel's drm/exynos device driver in exynos_drm_crtc_atomic_disable() function. This can result in a null pointer dereference issue, possibly leading to a kernel panic or denial of service issue.	2024-02-05	4.7	CVE-2024-22386
linux -- kernel	A race condition was found in the Linux kernel's sound/hda device driver in snd_hdac_regmap_sync() function. This can result in a null pointer dereference issue, possibly leading to a kernel panic or denial of service issue.	2024-02-05	4.7	CVE-2024-23196
linux -- kernel	A race condition was found in the Linux kernel's scsi device driver in lpfc_unregister_fcf_rescan() function. This can result in a null pointer dereference issue, possibly leading to a kernel panic or denial of service issue.	2024-02-05	4.7	CVE-2024-24855
linux -- kernel	A race condition was found in the Linux kernel's net/bluetooth in sniff_{min,max}_interval_set() function. This can result in a bluetooth sniffing exception issue, possibly leading denial of service.	2024-02-05	4.8	CVE-2024-24859
linux -- kernel	A race condition was found in the Linux kernel's bluetooth device driver in {min,max}_key_size_set() function. This can result in a null pointer dereference issue, possibly leading to a kernel panic or denial of service issue.	2024-02-05	4.6	CVE-2024-24860
linux -- kernel	A race condition was found in the Linux kernel's media/dvb-core in dvbdmx_write() function. This can result in a null pointer dereference issue, possibly leading to a kernel panic or denial of service issue.	2024-02-05	4.7	CVE-2024-24864
lê_văn_toản -- woocommerce_vietnam_checkout	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Lê Văn Toản Woocommerce Vietnam Checkout allows Stored XSS.This issue affects Woocommerce Vietnam Checkout: from n/a through 2.0.7.	2024-02-08	5.9	CVE-2024-24885
m2crypto -- m2crypto	A flaw was found in m2crypto. This issue may allow a remote attacker to decrypt captured messages in TLS servers that use RSA key exchanges, which may lead to exposure of confidential or sensitive data.	2024-02-05	5.9	CVE-2023-50781
mark_kinchin -- beds24_online_booking	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mark Kinchin Beds24 Online Booking allows Stored XSS. This issue affects Beds24 Online Booking: from n/a through 2.0.23.	2024-02-10	5.9	CVE-2024-24717

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mattermost -- mattermost	Mattermost fails to check if a custom emoji reaction exists when sending it to a post and to limit the amount of custom emojis allowed to be added in a post, allowing an attacker sending a huge amount of non-existent custom emojis in a post to crash the mobile app of a user seeing the post.	2024-02-09	4.3	CVE-2024-1402
michael_dempfle -- advanced_iframe	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michael Dempfle Advanced iFrame allows Stored XSS. This issue affects Advanced iFrame: from n/a through 2023.10.	2024-02-05	6.5	CVE-2024-24870
micronaut-projects -- micronaut-core	Micronaut Framework is a modern, JVM-based, full stack Java framework designed for building modular, easily testable JVM applications with support for Java, Kotlin and the Groovy language. Enabled but unsecured management endpoints are susceptible to drive-by localhost attacks. While not typical of a production application, these attacks may have more impact on a development environment where such endpoints may be flipped on without much thought. A malicious/compromised website can make HTTP requests to `localhost`. Normally, such requests would trigger a CORS preflight check which would prevent the request; however, some requests are "simple" and do not require a preflight check. These endpoints, if enabled and not secured, are vulnerable to being triggered. Production environments typically disable unused endpoints and secure/restrict access to needed endpoints. A more likely victim is the developer in their local development host, who has enabled endpoints without security for the sake of easing development. This issue has been addressed in version 3.8.3. Users are advised to upgrade.	2024-02-09	5.1	CVE-2024-23639
mightythemes -- mighty_addons	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MightyThemes Mighty Addons for Elementor allows Reflected XSS.This issue affects Mighty Addons for Elementor: from n/a through 1.9.3.	2024-02-05	6.1	CVE-2024-24846
miraheze -- managewiki	ManageWiki is a MediaWiki extension allowing users to manage wikis. Special:ManageWiki does not escape escape interface messages on the `columns` and `help` keys on the form descriptor. An attacker may exploit this and would have a cross site scripting attack vector. Exploiting this on-wiki requires the `(editinterface)` right. Users should apply the code changes in commits `886cc6b94`, `2ef0f50880`, and `6942e8b2c` to resolve this vulnerability. There are no known workarounds for this vulnerability.	2024-02-09	6.5	CVE-2024-25109
miraheze -- wikidiscover	WikiDiscover is an extension designed for use with a CreateWiki managed farm to display wikis. On Special:WikiDiscover, the `Language::date` function is used when making the human-readable timestamp for inclusion on the wiki_creation column. This function uses interface messages to translate the names of months and days. It uses the `->text()` output mode, returning unescaped interface messages. Since the output is not escaped later, the unescaped interface message is included on the output, resulting in an XSS vulnerability. Exploiting this on-wiki requires the `(editinterface)` right. This vulnerability has been addressed in commit `267e763a0`. Users are advised to update their installations. There are no known workarounds for this vulnerability.	2024-02-08	4.9	CVE-2024-25107
mjssoftware -- sign_ups	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MJS Software PT Sign Ups - Beautiful volunteer sign ups and management made easy allows Stored XSS.This issue affects PT Sign Ups - Beautiful volunteer sign ups and management made easy: from n/a through 1.0.4.	2024-02-05	6.1	CVE-2024-24848
mozilla -- firefox	When a user scans a QR Code with the QR Code Scanner feature, the user is not prompted before being navigated to the page specified in the code. This may surprise the user and potentially direct them to unwanted content.	2024-02-05	6.1	CVE-2024-0953
mpedraza2020 -- intranet_del_monterroso	A vulnerability was found in mpedraza2020 Intranet del Monterroso up to 4.50.0. It has been classified as critical. This affects an unknown part of the file config/cargos.php. The manipulation of the argument dni_profe leads to sql	2024-02-04	5.5	CVE-2019-25159

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	injection. Upgrading to version 4.51.0 is able to address this issue. The identifier of the patch is 678190bee1dfd64b54a2b0e88abfd009e78adce8. It is recommended to upgrade the affected component. The identifier VDB-252717 was assigned to this vulnerability.			
mrcms -- mrcms	MRCMS 3.0 contains a Cross-Site Scripting (XSS) vulnerability via /admin/system/saveinfo.do.	2024-02-02	5.4	CVE-2024-24160
munsoft -- easy_archive_recovery	A vulnerability classified as problematic was found in Munsoft Easy Archive Recovery 2.0. This vulnerability affects unknown code of the component Registration Key Handler. The manipulation leads to denial of service. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252676. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-02	5.5	CVE-2024-1186
munsoft -- easy_outlook_express_recovery	A vulnerability, which was classified as problematic, has been found in Munsoft Easy Outlook Express Recovery 2.0. This issue affects some unknown processing of the component Registration Key Handler. The manipulation 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-252677 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-02	5.5	CVE-2024-1187
nagios -- nagios_xi	A stored cross-site scripting (XSS) vulnerability in the NOC component of Nagios XI version up to and including 2024R1 allows low-privileged users to execute malicious HTML or JavaScript code via the audio file upload functionality from the Operation Center section. This allows any authenticated user to execute arbitrary JavaScript code on behalf of other users, including the administrators.	2024-02-02	5.4	CVE-2023-51072
nationalkeep -- cybermath	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in National Keep Cyber Security Services CyberMath allows Reflected XSS.This issue affects CyberMath: from v.1.4 before v.1.5.	2024-02-02	6.1	CVE-2023-6673
nationalkeep -- cybermath	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in National Keep Cyber Security Services CyberMath allows Stored XSS.This issue affects CyberMath: from v1.4 before v1.5.	2024-02-02	5.4	CVE-2023-6672
navicat -- navicat	A vulnerability was found in Navicat 12.0.29. It has been rated as problematic. This issue affects some unknown processing of the component MySQL Conecction Handler. The manipulation leads to denial of service. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252683. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-02	5.5	CVE-2024-1193
netapp -- storagegrid_(formerly_storagegrid_webscale)	StorageGRID (formerly StorageGRID Webscale) versions 11.6.0 through 11.6.0.13 are susceptible to a Denial of Service (DoS) vulnerability. A successful exploit could lead to a crash of the Local Distribution Router (LDR) service.	2024-02-05	6.5	CVE-2023-27318
noahkagan -- scroll_triggered_box	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Noah Kagan Scroll Triggered Box allows Stored XSS.This issue affects Scroll Triggered Box: from n/a through 2.3.	2024-02-05	5.4	CVE-2024-24865
nonebot -- nonebot2	nonebot2 is a cross-platform Python asynchronous chatbot framework written in Python. This security advisory pertains to a potential information leak (e.g., environment variables) in instances where developers utilize `MessageTemplate` and incorporate user-provided data into templates. The identified vulnerability has been remedied in pull request #2509 and will be included in versions released from 2.2.0. Users are strongly advised to upgrade to these patched versions to safeguard against the vulnerability. A temporary workaround involves filtering underscores before incorporating user input into the message template.	2024-02-09	5.7	CVE-2024-21624

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nsasoft -- network_bandwidth_monitor	A vulnerability classified as problematic has been found in Nsasoft NBMonitor Network Bandwidth Monitor 1.6.5.0. This affects an unknown part of the component Registration Handler. The manipulation leads to denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252675. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-02	5.5	CVE-2024-1185
nsasoft -- network_sleuth	A vulnerability was found in Nsasoft Network Sleuth 3.0.0.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Registration Handler. The manipulation leads to denial of service. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. VDB-252674 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-02	5.5	CVE-2024-1184
openbi -- openbi	A vulnerability, which was classified as critical, was found in openBI up to 6.0.3. Affected is the function addxinzhi of the file application/controllers/User.php of the component Phar Handler. The manipulation of the argument outimgurl leads to deserialization. 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-252696.	2024-02-03	6.3	CVE-2024-1198
openharmony -- openharmony	in OpenHarmony v4.0.0 and prior versions allow a local attacker cause DOS through improper input.	2024-02-02	6.2	CVE-2024-21863
openharmony -- openharmony	in OpenHarmony v3.2.4 and prior versions allow a local attacker causes information leak through out-of-bounds Read.	2024-02-02	5.5	CVE-2023-43756
openharmony -- openharmony	in OpenHarmony v3.2.4 and prior versions allow a local attacker causes information leak through out-of-bounds Read.	2024-02-02	5.5	CVE-2023-49118
openharmony -- openharmony	in OpenHarmony v4.0.0 and prior versions allow a local attacker cause DOS through improper input.	2024-02-02	5.5	CVE-2024-0285
phpems -- phpems	A vulnerability, which was classified as critical, has been found in PHPEMS up to 1.0. Affected by this issue is the function index of the file app/weixin/controller/index.api.php. The manipulation of the argument picurl leads to deserialization. The exploit has been disclosed to the public and may be used. VDB-253226 is the identifier assigned to this vulnerability.	2024-02-09	6.3	CVE-2024-1353
pimcore -- admin_ui_classic_bundle	Pimcore's Admin Classic Bundle provides a backend user interface for Pimcore. Prior to version 1.3.3, an attacker can create, delete etc. tags without having the permission to do so. A fix is available in version 1.3.3. As a workaround, one may apply the patch manually.	2024-02-07	6.5	CVE-2024-24822
plotly -- dash	Versions of the package dash-core-components before 2.13.0; all versions of the package dash-core-components; versions of the package dash before 2.15.0; all versions of the package dash-html-components; versions of the package dash-html-components before 2.0.16 are vulnerable to Cross-site Scripting (XSS) when the href of the a tag is controlled by an adversary. An authenticated attacker who stores a view that exploits this vulnerability could steal the data that's visible to another user who opens that view - not just the data already included on the page, but they could also, in theory, make additional requests and access other data accessible to this user. In some cases, they could also steal the access tokens of that user, which would allow the attacker to act as that user, including viewing other apps and resources hosted on the same server. **Note:** This is only exploitable in Dash apps that include some mechanism to store user input to be reloaded by a different user.	2024-02-02	5.4	CVE-2024-21485
pyload -- pyload	pyLoad is an open-source Download Manager written in pure Python. There is an open redirect vulnerability due to incorrect validation of input values when	2024-02-06	4.7	CVE-2024-24808

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	redirecting users after login. pyLoad is validating URLs via the `get_redirect_url` function when redirecting users at login. This vulnerability has been patched with commit fe94451.			
python -- cryptography	A flaw was found in the python-cryptography package. This issue may allow a remote attacker to decrypt captured messages in TLS servers that use RSA key exchanges, which may lead to exposure of confidential or sensitive data.	2024-02-05	5.9	CVE-2023-50782
qnap -- photo_station	A cross-site scripting (XSS) vulnerability has been reported to affect Photo Station. 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: Photo Station 6.4.2 (2023/12/15) and later	2024-02-02	5.4	CVE-2023-47561
qnap -- qts	An incorrect authorization vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to bypass intended access restrictions via a network. QTS 5.x, QuTS hero are not affected. We have already fixed the vulnerability in the following versions: QuTScloud c5.1.5.2651 and later QTS 4.5.4.2627 build 20231225 and later	2024-02-02	6.5	CVE-2023-32967
qnap -- qts	An unchecked return value vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow local authenticated administrators to place the system in a state that could lead to a crash or other unintended behaviors via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.5.2645 build 20240116 and later QuTS hero h5.1.5.2647 build 20240118 and later	2024-02-02	6.7	CVE-2023-50359
qnap -- qts	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.2.2533 build 20230926 and later QuTS hero h5.1.2.2534 build 20230927 and later QuTScloud c5.1.5.2651 and later	2024-02-02	4.9	CVE-2023-41274
qnap -- qts	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.5.2645 build 20240116 and later QuTS hero h5.1.5.2647 build 20240118 and later QuTScloud c5.1.5.2651 and later	2024-02-02	4.9	CVE-2023-45026
qnap -- qts	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.5.2645 build 20240116 and later QuTS hero h5.1.5.2647 build 20240118 and later QuTScloud c5.1.5.2651 and later	2024-02-02	4.9	CVE-2023-45027
qnap -- qts	An uncontrolled resource consumption vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.5.2645 build 20240116 and later QuTS hero h5.1.5.2647 build 20240118 and later QuTScloud c5.1.5.2651 and later	2024-02-02	4.9	CVE-2023-45028
qualcomm -- aqt1000_firmware	Transient DOS in Audio when invoking callback function of ASM driver.	2024-02-06	5.5	CVE-2023-33064
qualcomm -- ar8035_firmware	Transient DOS in Core when DDR memory check is called while DDR is not initialized.	2024-02-06	5.5	CVE-2023-33060

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rapidscada -- rapid_scada	In Rapid Software LLC's Rapid SCADA versions prior to Version 5.8.4, an attacker can append path traversal characters to the filename when using a specific command, allowing them to read arbitrary files from the system.	2024-02-02	6.5	CVE-2024-22096
rapidscada -- rapid_scada	In Rapid Software LLC's Rapid SCADA versions prior to Version 5.8.4, an attacker can redirect users to malicious pages through the login page.	2024-02-02	5.4	CVE-2024-21794
rapidscada -- rapid_scada	In Rapid Software LLC's Rapid SCADA versions prior to Version 5.8.4, the affected product responds back with an error message containing sensitive data if it receives a specific malformed request.	2024-02-02	5.3	CVE-2024-21866
rapidscada -- rapid_scada	In Rapid Software LLC's Rapid SCADA versions prior to Version 5.8.4, the affected product stores plaintext credentials in various places. This may allow an attacker with local access to see them.	2024-02-02	5.5	CVE-2024-21869
rdkcentral -- rdk-b	In da, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08477148; Issue ID: ALPS08477148.	2024-02-05	6.7	CVE-2024-20006
realmag777 -- active_products_tables_for_woocommerce_professional_products_tables_for_woocommerce_store	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in realmag777 Active Products Tables for WooCommerce. Professional products tables for WooCommerce store allows Stored XSS.This issue affects Active Products Tables for WooCommerce. Professional products tables for WooCommerce store: from n/a through 1.0.6.	2024-02-10	6.5	CVE-2023-51480
realmag777 -- bear_bulk_editor_and_products_manager_professional_for_woocommerce_by_pluginus.net	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in realmag777 BEAR - Bulk Editor and Products Manager Professional for WooCommerce by Pluginus.Net allows Stored XSS.This issue affects BEAR - Bulk Editor and Products Manager Professional for WooCommerce by Pluginus.Net: from n/a through 1.1.4.	2024-02-08	5.9	CVE-2024-24834
remyandrade -- testimonial_page_manager	A vulnerability classified as problematic was found in SourceCodester Testimonial Page Manager 1.0. This vulnerability affects unknown code of the file add-testimonial.php of the component HTTP POST Request Handler. The manipulation of the argument name/description/testimony leads to cross site scripting. The attack can be initiated remotely. VDB-252694 is the identifier assigned to this vulnerability.	2024-02-02	6.1	CVE-2024-1196
rizonesoft -- notepad3	A vulnerability, which was classified as problematic, was found in Rizone Soft Notepad3 1.0.2.350. Affected is an unknown function of the component Encryption Passphrase Handler. The manipulation leads to denial of service. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. VDB-252678 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-02	5.5	CVE-2024-1188
samsung -- galaxy_store	Implicit intent hijacking vulnerability in AccountActivity of Galaxy Store prior to version 4.5.63.6 allows local attackers to access sensitive information via implicit intent.	2024-02-06	5.5	CVE-2024-20822
samsung -- galaxy_store	Implicit intent hijacking vulnerability in SamsungAccount of Galaxy Store prior to version 4.5.63.6 allows local attackers to access sensitive information via implicit intent.	2024-02-06	5.5	CVE-2024-20823
samsung -- galaxy_store	Implicit intent hijacking vulnerability in VoiceSearch of Galaxy Store prior to version 4.5.63.6 allows local attackers to access sensitive information via implicit intent.	2024-02-06	5.5	CVE-2024-20824
samsung -- galaxy_store	Implicit intent hijacking vulnerability in IAP of Galaxy Store prior to version 4.5.63.6 allows local attackers to access sensitive information via implicit intent.	2024-02-06	5.5	CVE-2024-20825

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
samsung_mobile -- samsung_mobile_devices	Out bounds Write vulnerabilities in svc1td_vld_slh of libsthmbc.so prior to SMR Feb-2024 Release 1 allows local attackers to trigger buffer overflow.	2024-02-06	6.6	CVE-2024-20817
samsung_mobile -- samsung_mobile_devices	Out bounds Write vulnerabilities in svc1td_vld_elh of libsthmbc.so prior to SMR Feb-2024 Release 1 allows local attackers to trigger buffer overflow.	2024-02-06	6.6	CVE-2024-20818
samsung_mobile -- samsung_mobile_devices	Out bounds Write vulnerabilities in svc1td_vld_plh_ap of libsthmbc.so prior to SMR Feb-2024 Release 1 allows local attackers to trigger buffer overflow.	2024-02-06	6.6	CVE-2024-20819
samsung_mobile -- samsung_mobile_devices	Improper caller verification in GameOptimizer prior to SMR Feb-2024 Release 1 allows local attackers to configure GameOptimizer.	2024-02-06	5.1	CVE-2024-20811
samsung_mobile -- samsung_mobile_devices	Out-of-bounds Read in padmd_vld_ac_prog_refine of libpadm.so prior to SMR Feb-2024 Release 1 allows attacker access unauthorized information.	2024-02-06	4	CVE-2024-20814
samsung_mobile -- samsung_mobile_devices	Improper input validation in bootloader prior to SMR Feb-2024 Release 1 allows attacker to cause an Out-Of-Bounds read.	2024-02-06	4.4	CVE-2024-20820
samsung_mobile -- samsung_mobile_devices	Improper access control vulnerability in Samsung Gallery prior to version 14.5.04.4 allows physical attackers to access the picture using physical keyboard on the lockscreen.	2024-02-06	4.6	CVE-2024-20827
samsung_mobile -- uphelper	Implicit intent hijacking vulnerability in UPHelper library prior to version 4.0.0 allows local attackers to access sensitive information via implicit intent.	2024-02-06	5.5	CVE-2024-20826
sepidz -- sepidzdigitalmenu	A vulnerability has been found in sepidz SepidzDigitalMenu up to 7.1.0728.1 and classified as problematic. This vulnerability affects unknown code of the file /Waiters. The manipulation leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-252994 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-06	5.3	CVE-2024-1255
snow_software -- snow_inventory_agent	Authentication Bypass by Spoofing vulnerability in Snow Software Snow Inventory Agent on Windows allows Signature Spoof. This issue affects Snow Inventory Agent: through 6.14.5. Customers advised to upgrade to version 7.0	2024-02-08	6	CVE-2023-7169
solar-log -- 2000_pm\+_firmware	A vulnerability in Solar-Log Base 15 Firmware 6.0.1 Build 161, and possibly other Solar-Log Base products, allows an attacker to escalate their privileges by exploiting a stored cross-site scripting (XSS) vulnerability in the switch group function under /#ilang=DE&b=c_smartenergy_swgroups in the web portal. The vulnerability can be exploited to gain the rights of an installer or PM, which can then be used to gain administrative access to the web portal and execute further attacks.	2024-02-02	5.4	CVE-2023-46344
spring_security -- spring_security	The spring-security.xsd file inside the spring-security-config jar is world writable which means that if it were extracted it could be written by anyone with access to the file system. While there are no known exploits, this is an example of "CWE-732: Incorrect Permission Assignment for Critical Resource" and could result in an exploit. Users should update to the latest version of Spring Security to mitigate any future exploits found around this issue.	2024-02-05	4.1	CVE-2023-34042
stimulsoft -- dashboards	Cross Site Scripting vulnerability in Stimulsoft GmbH Stimulsoft Dashboard.JS before v.2024.1.2 allows a remote attacker to execute arbitrary code via a crafted payload to the ReportName field.	2024-02-05	5.4	CVE-2024-24397

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
suite_crm -- suite_crm	Suite CRM version 7.14.2 allows making arbitrary HTTP requests through the vulnerable server. This is possible because the application is vulnerable to SSRF.	2024-02-07	5	CVE-2023-6388
tenable -- nessus	A SQL injection vulnerability exists where an authenticated, low-privileged remote attacker could potentially alter scan DB content.	2024-02-07	6.5	CVE-2024-0971
tenable -- nessus	A stored XSS vulnerability exists where an authenticated, remote attacker with administrator privileges on the Nessus application could alter Nessus proxy settings, which could lead to the execution of remote arbitrary scripts.	2024-02-07	4.8	CVE-2024-0955
thorsten -- phpmyfaq	phpMyFAQ is an Open Source FAQ web application for PHP 8.1+ and MySQL, PostgreSQL and other databases. The 'sharing FAQ' functionality allows any unauthenticated actor to misuse the phpMyFAQ application to send arbitrary emails to a large range of targets. The phpMyFAQ application has a functionality where anyone can share a FAQ item to others. The front-end of this functionality allows any phpMyFAQ articles to be shared with 5 email addresses. Any unauthenticated actor can perform this action. There is a CAPTCHA in place, however the amount of people you email with a single request is not limited to 5 by the backend. An attacker can thus solve a single CAPTCHA and send thousands of emails at once. An attacker can utilize the target application's email server to send phishing messages. This can get the server on a blacklist, causing all emails to end up in spam. It can also lead to reputation damages. This issue has been patched in version 3.2.5.	2024-02-05	6.5	CVE-2024-22208
thorsten -- phpmyfaq	phpMyFAQ is an open source FAQ web application for PHP 8.1+ and MySQL, PostgreSQL and other databases. Unsafe echo of filename in phpMyFAQ\phpmyfaq\admin\attachments.php leads to allowed execution of JavaScript code in client side (XSS). This vulnerability has been patched in version 3.2.5.	2024-02-05	6.5	CVE-2024-24574
thorsten -- phpmyfaq	phpMyFAQ is an open source FAQ web application for PHP 8.1+ and MySQL, PostgreSQL and other databases. phpMyFAQ's user removal page allows an attacker to spoof another user's detail, and in turn make a compelling phishing case for removing another user's account. The front-end of this page doesn't allow changing the form details, an attacker can utilize a proxy to intercept this request and submit other data. Upon submitting this form, an email is sent to the administrator informing them that this user wants to delete their account. An administrator has no way of telling the difference between the actual user wishing to delete their account or the attacker issuing this for an account they do not control. This issue has been patched in version 3.2.5.	2024-02-05	5.7	CVE-2024-22202
tongda -- oa_2017	A vulnerability classified as critical has been found in Tongda OA 2017 up to 11.10. Affected is an unknown function of the file /general/email/outbox/delete.php. The manipulation of the argument DELETE_STR leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-252990 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-06	5.5	CVE-2024-1251
tongda -- oa_2017	A vulnerability classified as critical was found in Tongda OA 2017 up to 11.9. Affected by this vulnerability is an unknown functionality of the file /general/attendance/manage/ask_duty/delete.php. The manipulation of the argument ASK_DUTY_ID 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 this vulnerability is VDB-252991.	2024-02-06	5.5	CVE-2024-1252
ujcms -- jspxcms	A vulnerability was found in Jspxcms 10.2.0. It has been classified as problematic. Affected is an unknown function of the file /ext/collect/find_text.do. 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-252996.	2024-02-06	6.1	CVE-2024-1257

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ujcms -- jspxcms	A vulnerability was found in Jspxcms 10.2.0 and classified as problematic. This issue affects some unknown processing of the file /ext/collect/filter_text.do. The manipulation 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-252995.	2024-02-06	4.3	CVE-2024-1256
vercel -- pkg	pkg is tool design to bundle Node.js projects into an executables. Any native code packages built by `pkg` are written to a hardcoded directory. On unix systems, this is `/tmp/pkg/*` which is a shared directory for all users on the same local system. There is no uniqueness to the package names within this directory, they are predictable. An attacker who has access to the same local system has the ability to replace the genuine executables in the shared directory with malicious executables of the same name. A user may then run the malicious executable without realising it has been modified. This package is deprecated. Therefore, there will not be a patch provided for this vulnerability. To check if your executable build by pkg depends on native code and is vulnerable, run the executable and check if `/tmp/pkg/` was created. Users should transition to actively maintained alternatives. We would recommend investigating Node.js 21's support for single executable applications. Given the decision to deprecate the pkg package, there are no official workarounds or remediations provided by our team. Users should prioritize migrating to other packages that offer similar functionality with enhanced security.	2024-02-09	6.6	CVE-2024-24828
vmware -- aria_operations_for_networks	Aria Operations for Networks contains a cross site scripting vulnerability. A malicious actor with admin privileges may be able to inject malicious code into user profile configurations due to improper input sanitization.	2024-02-06	4.8	CVE-2024-22238
vmware -- aria_operations_for_networks	Aria Operations for Networks contains a local file read vulnerability. A malicious actor with admin privileges may exploit this vulnerability leading to unauthorized access to sensitive information.	2024-02-06	4.9	CVE-2024-22240
vmware -- aria_operations_for_networks	Aria Operations for Networks contains a cross site scripting vulnerability. A malicious actor with admin privileges can inject a malicious payload into the login banner and takeover the user account.	2024-02-06	4.8	CVE-2024-22241
websoudan -- mw_wp_form	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in websoudan MW WP Form allows Stored XSS. This issue affects MW WP Form: from n/a through 5.0.6.	2024-02-10	6.5	CVE-2024-24804
westermo -- lynx	A potential attacker with access to the Westermo Lynx device would be able to execute malicious code that could affect the correct functioning of the device.	2024-02-06	6.6	CVE-2023-45213
westermo -- lynx	An attacker with access to the Westermo Lynx web application that has the vulnerable software could introduce arbitrary JavaScript by injecting a cross-site scripting payload into the "forward.0.domain" parameter.	2024-02-06	5.4	CVE-2023-40143
westermo -- lynx	An attacker with access to the network where the affected devices are located could maliciously actions to obtain, via a sniffer, sensitive information exchanged via TCP communications.	2024-02-06	5.7	CVE-2023-40544
westermo -- lynx	An attacker with access to the vulnerable software could introduce arbitrary JavaScript by injecting a cross-site scripting payload into the "username" parameter in the SNMP configuration.	2024-02-06	5.4	CVE-2023-42765
westermo -- lynx	An attacker with access to the web application that has the vulnerable software could introduce arbitrary JavaScript by injecting a cross-site scripting payload into the "autorefresh" parameter.	2024-02-06	5.4	CVE-2023-45222
westermo -- lynx	An attacker with access to the web application with vulnerable software could introduce arbitrary JavaScript by injecting a cross-site scripting payload into the "dns.0.server" parameter.	2024-02-06	5.4	CVE-2023-45227

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
western_digital -- my_cloud_os_5	Server-side request forgery (SSRF) vulnerability that could allow a rogue server on the local network to modify its URL using another DNS address to point back to the loopback adapter. This could then allow the URL to exploit other vulnerabilities on the local server. This was addressed by fixing DNS addresses that refer to loopback. This issue affects My Cloud OS 5 devices before 5.27.161, My Cloud Home, My Cloud Home Duo and SanDisk ibi devices before 9.5.1-104.	2024-02-05	5.5	CVE-2023-22817
western_digital -- my_cloud_os_5	An uncontrolled resource consumption vulnerability issue that could arise by sending crafted requests to a service to consume a large amount of memory, eventually resulting in the service being stopped and restarted was discovered in Western Digital My Cloud Home, My Cloud Home Duo, SanDisk ibi and Western Digital My Cloud OS 5 devices. This issue requires the attacker to already have root privileges in order to exploit this vulnerability. This issue affects My Cloud Home and My Cloud Home Duo: before 9.5.1-104; ibi: before 9.5.1-104; My Cloud OS 5: before 5.27.161.	2024-02-05	4.9	CVE-2023-22819
wolfssl -- wolfssl	wolfSSL SP Math All RSA implementation is vulnerable to the Marvin Attack, new variation of a timing Bleichenbacher style attack, when built with the following options to configure: --enable-all CFLAGS="-DWOLFSSL_STATIC_RSA" The define "WOLFSSL_STATIC_RSA" enables static RSA cipher suites, which is not recommended, and has been disabled by default since wolfSSL 3.6.6. Therefore the default build since 3.6.6, even with "--enable-all", is not vulnerable to the Marvin Attack. The vulnerability is specific to static RSA cipher suites, and expected to be padding-independent. The vulnerability allows an attacker to decrypt ciphertexts and forge signatures after probing with a large number of test observations. However, the server's private key is not exposed.	2024-02-09	5.9	CVE-2023-6935
wordpress -- wordpress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MyAgilePrivacy My Agile Privacy - The only GDPR solution for WordPress that you can truly trust allows Stored XSS.This issue affects My Agile Privacy - The only GDPR solution for WordPress that you can truly trust: from n/a through 2.1.7.	2024-02-10	6.5	CVE-2023-51404
wordpress -- wordpress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GiveWP GiveWP - Donation Plugin and Fundraising Platform allows Stored XSS.This issue affects GiveWP - Donation Plugin and Fundraising Platform: from n/a through 3.2.2.	2024-02-10	6.5	CVE-2023-51415
wordpress -- wordpress	The Payment Forms for Paystack plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcodes in all versions up to, and including, 3.4.1 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.	2024-02-08	6.4	CVE-2023-5665
wordpress -- wordpress	The Meta Box - WordPress Custom Fields Framework plugin for WordPress is vulnerable to Stored Cross-Site Scripting via custom post meta values displayed through the plugin's shortcode in all versions up to, and including, 5.9.2 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.	2024-02-05	6.4	CVE-2023-6526
wordpress -- wordpress	The Display custom fields in the frontend - Post and User Profile Fields plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode and postmeta in all versions up to, and including, 1.2.1 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	2024-02-05	6.4	CVE-2023-6982

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
wordpress -- wordpress	The 10Web AI Assistant - AI content writing assistant plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the install_plugin AJAX action in all versions up to, and including, 1.0.18. This makes it possible for authenticated attackers, with subscriber-level access and above, to install arbitrary plugins that can be used to gain further access to a compromised site.	2024-02-05	6.5	CVE-2023-6985
wordpress -- wordpress	The WordPress Button Plugin MaxButtons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including 9.7.6 due to insufficient input sanitization and output escaping on user supplied attributes. 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: This vulnerability was partially fixed in version 9.7.6.	2024-02-05	6.4	CVE-2023-7029
wordpress -- wordpress	The (Simply) Guest Author Name plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's post meta in all versions up to, and including, 4.34 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.	2024-02-05	6.4	CVE-2024-0254
wordpress -- wordpress	The Starbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Profile Display Name and Social Settings in all versions up to, and including, 3.4.8 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.	2024-02-07	6.4	CVE-2024-0256
wordpress -- wordpress	The Elementor Addons by Livemesh plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widget URL parameters in all versions up to, and including, 8.3.1 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.	2024-02-05	6.4	CVE-2024-0448
wordpress -- wordpress	The Orbit Fox by ThemeIsle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Pricing Table Elementor Widget in all versions up to, and including, 2.10.27 due to insufficient input sanitization and output escaping on the user supplied link URL. 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.	2024-02-05	6.4	CVE-2024-0508
wordpress -- wordpress	The WP 404 Auto Redirect to Similar Post plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'request' parameter in all versions up to, and including, 1.0.3 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.	2024-02-05	6.1	CVE-2024-0509
wordpress -- wordpress	The Essential Addons for Elementor - Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Login/Register Element in all versions up to, and including, 5.9.4 due to insufficient input sanitization and output escaping on the custom login URL. 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.	2024-02-05	6.5	CVE-2024-0586

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 Cross-Site Request Forgery in all versions up to, and including, 6.7.2. This is due to missing or incorrect nonce validation on the update_settings function. This makes it possible for unauthenticated attackers to change form settings and add malicious JavaScript via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-02-05	6.1	CVE-2024-0660
wordpress -- wordpress	The Advanced Database Cleaner plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.1.3 via deserialization of untrusted input in the 'process_bulk_action' function. This makes it possible for authenticated attacker, with administrator access and above, to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	2024-02-05	6.6	CVE-2024-0668
wordpress -- wordpress	The Order Delivery Date for WP e-Commerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'available-days-tf' parameter in all versions up to, and including, 1.2 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.	2024-02-05	6.5	CVE-2024-0678
wordpress -- wordpress	The AI Engine: Chatbots, Generators, Assistants, GPT 4 and more! plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'add_image_from_url' function in all versions up to, and including, 2.1.4. This makes it possible for authenticated attackers, with Editor access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-02-05	6.6	CVE-2024-0699
wordpress -- wordpress	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the link_to parameter in all versions up to, and including, 1.12.11 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.	2024-02-05	6.4	CVE-2024-0834
wordpress -- wordpress	The Essential Addons for Elementor - Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting through editing context via the 'data-eael-wrapper-link' wrapper in all versions up to, and including, 5.9.7 due to insufficient input sanitization and output escaping on user supplied protocols. 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.	2024-02-05	6.4	CVE-2024-0954
wordpress -- wordpress	The SiteOrigin Widgets Bundle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the code editor in all versions up to, and including, 1.58.1 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.	2024-02-05	6.4	CVE-2024-0961
wordpress -- wordpress	The All-In-One Security (AIOS) - Security and Firewall plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in all versions up to, and including, 5.2.5 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.	2024-02-07	6.1	CVE-2024-1037
wordpress -- wordpress	The Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content - ProfilePress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin 'reg-number-field' shortcode in all versions up to, and including, 4.14.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for	2024-02-05	6.4	CVE-2024-1046

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			
wordpress -- wordpress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Calculators World CC BMI Calculator allows Stored XSS. This issue affects CC BMI Calculator: from n/a through 2.0.1.	2024-02-10	6.5	CVE-2024-23516
wordpress -- wordpress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Start Booking Scheduling Plugin - Online Booking for WordPress allows Stored XSS. This issue affects Scheduling Plugin - Online Booking for WordPress: from n/a through 3.5.10.	2024-02-10	6.5	CVE-2024-23517
wordpress -- wordpress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Team Heateor Heateor Social Login WordPress allows Stored XSS. This issue affects Heateor Social Login WordPress: from n/a through 1.1.30.	2024-02-10	6.5	CVE-2024-24712
wordpress -- wordpress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Auto Listings Auto Listings - Car Listings & Car Dealership Plugin for WordPress allows Stored XSS. This issue affects Auto Listings - Car Listings & Car Dealership Plugin for WordPress: from n/a through 2.6.5.	2024-02-10	6.5	CVE-2024-24713
wordpress -- wordpress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LogicHunt OWL Carousel - WordPress Owl Carousel Slider allows Stored XSS. This issue affects OWL Carousel - WordPress Owl Carousel Slider: from n/a through 1.4.0.	2024-02-10	6.5	CVE-2024-24801
wordpress -- wordpress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPoperation Ultra Companion - Companion plugin for WPoperation Themes allows Stored XSS. This issue affects Ultra Companion - Companion plugin for WPoperation Themes: from n/a through 1.1.9.	2024-02-10	6.5	CVE-2024-24803
wordpress -- wordpress	The Events Calendar plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 6.2.8.2 via the route function hooked into wp_ajax_nopriv_tribe_dropdown. This makes it possible for unauthenticated attackers to extract potentially sensitive data including post titles and IDs of pending, private and draft posts.	2024-02-05	5.3	CVE-2023-6557
wordpress -- wordpress	The Advanced Custom Fields (ACF) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via a custom text field in all versions up to, and including, 6.2.4 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.	2024-02-05	5.4	CVE-2023-6701
wordpress -- wordpress	The GeneratePress Premium plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's custom meta output in all versions up to, and including, 2.3.2 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.	2024-02-05	5.4	CVE-2023-6807
wordpress -- wordpress	The Booking for Appointments and Events Calendar - Amelia plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 1.0.93 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.	2024-02-05	5.4	CVE-2023-6808

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	This plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode in all versions up to, and including, 3.1 due to insufficient input sanitization and output escaping on the 'place_id' attribute. 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.	2024-02-05	5.4	CVE-2023-6884
wordpress -- wordpress	The Getwid - Gutenberg Blocks plugin for WordPress is vulnerable to CAPTCHA Bypass in versions up to, and including, 2.0.4. This makes it possible for unauthenticated attackers to bypass the Captcha Verification of the Contact Form block by omitting 'g-recaptcha-response' from the 'data' array.	2024-02-05	5.3	CVE-2023-6963
wordpress -- wordpress	The Author Box, Guest Author and Co-Authors for Your Posts - Molongui plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.7.4 via the 'ma_debu' parameter. This makes it possible for unauthenticated attackers to extract sensitive data including post author emails and names if applicable.	2024-02-05	5.3	CVE-2023-7014
wordpress -- wordpress	The WP Recipe Maker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wprm-recipe-text-share' shortcode 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.	2024-02-05	5.4	CVE-2024-0255
wordpress -- wordpress	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 unrestricted use of the 'header_tag' attribute. 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.	2024-02-05	5.4	CVE-2024-0382
wordpress -- wordpress	The WP Recipe Maker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Recipe Notes in all versions up to, and including, 9.1.0 due to insufficient input sanitization and output escaping. 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.	2024-02-05	5.4	CVE-2024-0384
wordpress -- wordpress	The Essential Addons for Elementor - Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Filterable Gallery widget in all versions up to, and including, 5.9.4 due to insufficient input sanitization and output escaping on the Image URL. 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.	2024-02-05	5.4	CVE-2024-0585
wordpress -- wordpress	The Awesome Support - WordPress HelpDesk & Support Plugin plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the editor_html() function in all versions up to, and including, 6.1.7. This makes it possible for authenticated attackers, with subscriber-level access and above, to view password protected and draft posts.	2024-02-10	5.3	CVE-2024-0596
wordpress -- wordpress	The Easy Digital Downloads - Sell Digital Files (eCommerce Store & Payments Made Easy) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the variable pricing option title in all versions up to, and including, 3.2.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with shop manger-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-02-05	5.5	CVE-2024-0659

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The FileBird plugin for WordPress is vulnerable to Stored Cross-Site Scripting via imported folder titles in all versions up to, and including, 5.5.8.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. It may also be possible to socially engineer an administrator into uploading a malicious folder import.	2024-02-05	5.5	CVE-2024-0691
wordpress -- wordpress	The UserPro plugin for WordPress is vulnerable to Security Feature Bypass in all versions up to, and including, 5.1.6. This is due to the use of client-side restrictions to enforce the 'Disabled registration' Membership feature within the plugin's General settings. This makes it possible for unauthenticated attackers to register an account even when account registration has been disabled by an administrator.	2024-02-05	5.3	CVE-2024-0701
wordpress -- wordpress	The WOLF - WordPress Posts Bulk Editor and Manager Professional plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.8.1. This is due to missing or incorrect nonce validation on the wpbe_create_new_term, wpbe_update_tax_term, and wpbe_delete_tax_term functions. This makes it possible for unauthenticated attackers to create, modify and delete taxonomy terms via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. Furthermore, the functions wpbe_save_options, wpbe_bulk_delete_posts_count, wpbe_bulk_delete_posts, and wpbe_save_meta are vulnerable to Cross-Site Request Forgery allowing for plugin options update, post count deletion, post deletion and modification of post metadata via forged request.	2024-02-05	5.4	CVE-2024-0790
wordpress -- wordpress	The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Link To' url in carousels in all versions up to, and including, 2.6.8 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.	2024-02-05	5.4	CVE-2024-0823
wordpress -- wordpress	The PDF Flipbook, 3D Flipbook - DearFlip plugin for WordPress is vulnerable to Stored Cross-Site Scripting via outline settings in all versions up to, and including, 2.2.26 due to insufficient input sanitization and output escaping on user supplied data. 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.	2024-02-03	5.4	CVE-2024-0895
wordpress -- wordpress	The Calculated Fields Form plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's CP_CALCULATED_FIELDS shortcode in all versions up to, and including, 1.2.52 due to insufficient input sanitization and output escaping on user supplied 'location' attribute. 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.	2024-02-02	5.4	CVE-2024-0963
wordpress -- wordpress	The Simple Page Access Restriction plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.0.21 via the REST API. This makes it possible for unauthenticated attackers to bypass the plugin's page restriction and view page content.	2024-02-08	5.3	CVE-2024-0965
wordpress -- wordpress	The ARMember plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.0.21 via the REST API. This makes it possible for unauthenticated attackers to bypass the plugin's "Default Restriction" feature and view restricted post content.	2024-02-05	5.3	CVE-2024-0969
wordpress -- wordpress	The Orbit Fox by ThemeIsle plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the register_reference() function in all versions up to, and including, 2.10.28. This makes it possible for unauthenticated attackers to update the connected API keys.	2024-02-02	5.3	CVE-2024-1047

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The PowerPack Addons for Elementor (Free Widgets, Extensions and Templates) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's buttons in all versions up to, and including, 2.7.14 due to insufficient input sanitization and output escaping on user supplied URL 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.	2024-02-07	5.4	CVE-2024-1055
wordpress -- wordpress	The SlimStat Analytics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'filter_array' parameter in all versions up to, and including, 5.1.3 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.	2024-02-02	5.4	CVE-2024-1073
wordpress -- wordpress	The Quiz Maker plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the ays_show_results() function in all versions up to, and including, 6.5.2.4. This makes it possible for unauthenticated attackers to fetch arbitrary quiz results which can contain PII.	2024-02-07	5.3	CVE-2024-1079
wordpress -- wordpress	The Podlove Podcast Publisher plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the init_download() and init() functions in all versions up to, and including, 4.0.11. This makes it possible for unauthenticated attackers to export the plugin's tracking data and podcast information.	2024-02-07	5.3	CVE-2024-1109
wordpress -- wordpress	The Podlove Podcast Publisher plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the init() function in all versions up to, and including, 4.0.11. This makes it possible for unauthenticated attackers to import the plugin's settings.	2024-02-07	5.3	CVE-2024-1110
wordpress -- wordpress	The Advanced Forms for ACF plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the export_json_file() function in all versions up to, and including, 1.9.3.2. This makes it possible for unauthenticated attackers to export form settings.	2024-02-05	5.3	CVE-2024-1121
wordpress -- wordpress	The Event Manager, Events Calendar, Events Tickets for WooCommerce - Eventin plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the export_data() function in all versions up to, and including, 3.3.50. This makes it possible for unauthenticated attackers to export event data.	2024-02-09	5.3	CVE-2024-1122
wordpress -- wordpress	The WP Club Manager - WordPress Sports Club Plugin plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the settings_save() function in all versions up to, and including, 2.2.10. This makes it possible for unauthenticated attackers to update the permalink structure for the clubs	2024-02-05	5.3	CVE-2024-1177
wordpress -- wordpress	The LearnDash LMS plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.10.2 via API. This makes it possible for unauthenticated attackers to obtain access to quiz questions.	2024-02-05	5.3	CVE-2024-1208
wordpress -- wordpress	The LearnDash LMS plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.10.1 via direct file access due to insufficient protection of uploaded assignments. This makes it possible for unauthenticated attackers to obtain those uploads.	2024-02-05	5.3	CVE-2024-1209
wordpress -- wordpress	The LearnDash LMS plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.10.1 via API. This makes it possible for unauthenticated attackers to obtain access to quizzes.	2024-02-05	5.3	CVE-2024-1210
wordpress -- wordpress	The WPvivid plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the restore() and get_restore_progress() function in versions up to, and including, 0.9.94. This makes it possible for unauthenticated	2024-02-05	4.3	CVE-2023-4637

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attackers to invoke these functions and obtain full file paths if they have access to a back-up ID.			
wordpress -- wordpress	The PDF Generator For Fluent Forms - The Contact Form Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the header, PDF body and footer content parameters in all versions up to, and including, 1.1.7 due to insufficient input sanitization and output escaping. This makes it possible for attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The exploitation level depends on who is granted the right to create forms by an administrator. This level can be as low as contributor, but by default is admin.	2024-02-05	4.9	CVE-2023-6953
wordpress -- wordpress	The Getwid - Gutenberg Blocks plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the recaptcha_api_key_manage function in all versions up to, and including, 2.0.3. This makes it possible for authenticated attackers, with subscriber-level access and above, to add, modify, or delete the 'Recaptcha Site Key' and 'Recaptcha Secret Key' settings.	2024-02-05	4.3	CVE-2023-6959
wordpress -- wordpress	The Display custom fields in the frontend - Post and User Profile Fields plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.2.1 via the vg_display_data shortcode due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with contributor-level access and above, to retrieve potentially sensitive post meta.	2024-02-05	4.3	CVE-2023-6983
wordpress -- wordpress	The Starbox - the Author Box for Humans plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.4.7 via the action function due to missing validation on a user controlled key. This makes it possible for subscribers to view plugin preferences and potentially other user settings.	2024-02-05	4.3	CVE-2024-0366
wordpress -- wordpress	The Views for WPForms - Display & Edit WPForms Entries on your site frontend plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'save_view' function in all versions up to, and including, 3.2.2. This makes it possible for authenticated attackers, with subscriber access and above, to modify the titles of arbitrary posts.	2024-02-05	4.3	CVE-2024-0370
wordpress -- wordpress	The Views for WPForms - Display & Edit WPForms Entries on your site frontend plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'create_view' function in all versions up to, and including, 3.2.2. This makes it possible for authenticated attackers, with subscriber access and above, to create form views.	2024-02-05	4.3	CVE-2024-0371
wordpress -- wordpress	The Views for WPForms - Display & Edit WPForms Entries on your site frontend plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'get_form_fields' function in all versions up to, and including, 3.2.2. This makes it possible for authenticated attackers, with subscriber access and above, to create form views.	2024-02-05	4.3	CVE-2024-0372
wordpress -- wordpress	The Views for WPForms - Display & Edit WPForms Entries on your site frontend plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.2.2. This is due to missing or incorrect nonce validation on the 'save_view' function. This makes it possible for unauthenticated attackers to modify arbitrary post titles via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-02-05	4.3	CVE-2024-0373
wordpress -- wordpress	The Views for WPForms - Display & Edit WPForms Entries on your site frontend plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.2.2. This is due to missing or incorrect nonce validation on the 'create_view' function. This makes it possible for unauthenticated attackers to	2024-02-05	4.3	CVE-2024-0374

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	create views via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.			
wordpress -- wordpress	The WP Recipe Maker plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 9.1.0 via the 'icon' attribute used in Shortcodes. This makes it possible for authenticated attackers, with contributor-level access and above, to include the contents of SVG files on the server, which can be leveraged for Cross-Site Scripting.	2024-02-05	4.3	CVE-2024-0380
wordpress -- wordpress	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.3.87. This is due to missing or incorrect nonce validation on the wpr_update_form_action_meta function. This makes it possible for unauthenticated attackers to post metadata via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-02-08	4.3	CVE-2024-0511
wordpress -- wordpress	The Awesome Support - WordPress HelpDesk & Support Plugin plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the wpas_get_users() function hooked via AJAX in all versions up to, and including, 6.1.7. This makes it possible for authenticated attackers, with subscriber-level access and above, to retrieve user data such as emails.	2024-02-10	4.3	CVE-2024-0595
wordpress -- wordpress	The SEO Plugin by Squirrly SEO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to and including 12.3.15 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.	2024-02-05	4.4	CVE-2024-0597
wordpress -- wordpress	The Content Views - Post Grid, Slider, Accordion (Gutenberg Blocks and Shortcode) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.6.2 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.	2024-02-05	4.4	CVE-2024-0612
wordpress -- wordpress	The WP RSS Aggregator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the RSS feed source in all versions up to, and including, 4.23.4 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.	2024-02-05	4.4	CVE-2024-0630
wordpress -- wordpress	The Internal Link Juicer: SEO Auto Linker for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings such as 'ilj_settings_field_links_per_page' in all versions up to, and including, 2.23.4 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.	2024-02-09	4.4	CVE-2024-0657
wordpress -- wordpress	The WOLF - WordPress Posts Bulk Editor and Manager Professional plugin for WordPress is vulnerable to unauthorized access, modification or loss of data due to a missing capability check on the wpbe_create_new_term, wpbe_update_tax_term, and wpbe_delete_tax_term functions in all versions up to, and including, 1.0.8.1. This makes it possible for authenticated attackers, with subscriber access or higher, to create, delete or modify taxonomy terms.	2024-02-05	4.3	CVE-2024-0791

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Active Products Tables for WooCommerce. Professional products tables for WooCommerce store plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.6.1. This is due to missing or incorrect nonce validation on several functions corresponding to AJAX actions. This makes it possible for unauthenticated attackers to invoke those functions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-02-05	4.3	CVE-2024-0796
wordpress -- wordpress	The Active Products Tables for WooCommerce. Professional products tables for WooCommerce store plugin for WordPress is vulnerable to unauthorized access of functionality due to a missing capability check on several functions in all versions up to, and including, 1.0.6.1. This makes it possible for subscribers and higher to execute functions intended for admin use.	2024-02-05	4.3	CVE-2024-0797
wordpress -- wordpress	The Royal Elementor Kit theme for WordPress is vulnerable to unauthorized arbitrary transient update due to a missing capability check on the dismissed_handler function in all versions up to, and including, 1.0.116. This makes it possible for authenticated attackers, with subscriber access or higher, to update arbitrary transients. Note, that these transients can only be updated to true and not arbitrary values.	2024-02-05	4.3	CVE-2024-0835
wordpress -- wordpress	The Affiliates Manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.9.34. This is due to missing or incorrect nonce validation on the process_bulk_action function in ListAffiliatesTable.php. This makes it possible for unauthenticated attackers to delete affiliates via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-02-05	4.3	CVE-2024-0859
wordpress -- wordpress	The Timeline Widget For Elementor (Elementor Timeline, Vertical & Horizontal Timeline) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via image URLs in the plugin's timeline widget in all versions up to, and including, 1.5.3 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, changes the slideshow type, and then changes it back to an image.	2024-02-07	4.4	CVE-2024-0977
wordpress -- wordpress	The Quiz Maker plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the ays_quick_start() and add_question_rows() functions in all versions up to, and including, 6.5.2.4. This makes it possible for authenticated attackers, with subscriber-level access and above, to create arbitrary quizzes.	2024-02-07	4.3	CVE-2024-1078
wordpress -- wordpress	The RSS Aggregator by Feedzy - Feed to Post, Autoblogging, News & YouTube Video Feeds Aggregator plugin for WordPress is vulnerable to unauthorized data modification due to a missing capability check on the feedzy dashboard in all versions up to, and including, 4.4.1. This makes it possible for authenticated attackers, with contributor access or higher, to create, edit or delete feed categories created by them.	2024-02-05	4.3	CVE-2024-1092
wordpress -- wordpress	The Orbit Fox by ThemeIsle plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.10.29. This is due to missing or incorrect nonce validation on the register_reference() function. This makes it possible for unauthenticated attackers to update the connected API keys via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-02-02	4.3	CVE-2024-1162
wp_hosting -- pay_with_vipps_and_mobilepay_for_woocommerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Hosting Pay with Vipps and MobilePay for WooCommerce allows Stored XSS. This issue affects Pay with Vipps and MobilePay for WooCommerce: from n/a through 1.14.13.	2024-02-10	6.5	CVE-2023-51485

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wpsc-plugin -- structured_content	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Gordon Böhme, Antonio Leutsch Structured Content (JSON-LD) #wpsc allows Stored XSS.This issue affects Structured Content (JSON-LD) #wpsc: from n/a through 1.6.1.	2024-02-05	5.4	CVE-2024-24839
xunruicms -- xunruicms	Cross-site scripting (XSS) vulnerability in XunRuiCMS versions v4.6.2 and before, allows remote attackers to obtain sensitive information via crafted malicious requests to the background login.	2024-02-02	6.1	CVE-2024-24388
zabbix -- zabbix	The cause of vulnerability is improper validation of form input field "Name" on Graph page in Items section.	2024-02-09	5.5	CVE-2024-22119 security@zabbix.com

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ZhongBangKeJi -- cremeb	A vulnerability was found in ZhongBangKeJi CRMEB 5.2.2. It has been classified as problematic. This affects the function openfile of the file /adminapi/system/file/openfile. The manipulation leads to absolute path traversal. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-254391. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-21	3.5	CVE-2024-1703
ZhongBangKeJi -- cremeb	A vulnerability, which was classified as problematic, has been found in ZKTeco ZKBio Access IVS up to 3.3.2. Affected by this issue is some unknown functionality of the component Department Name Search Bar. The manipulation with the input <marquee>hi leads to cross site scripting. 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-254396. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-21	3.5	CVE-2024-1706
alfio-event -- alf.io	Alf.io is a free and open source event attendance management system. An administrator on the alf.io application is able to upload HTML files that trigger JavaScript payloads. As such, an attacker gaining administrative access to the alf.io application may be able to persist access by planting an XSS payload. This issue has been addressed in version 2.0-M4-2402. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-16	3.5	CVE-2024-25627
bdtask -- bhojon_best_restaurant_management_software	A vulnerability, which was classified as problematic, has been found in Bdtask Bhojon Best Restaurant Management Software 2.9. This issue affects some unknown processing of the file /dashboard/message of the component Message Page. The manipulation of the argument Title 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-254531. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-22	2.4	CVE-2024-1749
beyondtrust -- privilege_management_for_windows	Prior to version 24.1, a local authenticated attacker can view Sysvol when Privilege Management for Windows is configured to use a GPO policy. This allows them to view the policy and potentially find configuration issues.	2024-02-16	3.3	CVE-2024-1591 13061848-ea10-403d-bd75-c83a022c2891
github -- codeql-cli-binaries	The CodeQL CLI repo holds binaries for the CodeQL command line interface (CLI). Prior to version 2.16.3, an XML parser used by the CodeQL CLI to read various auxiliary files is vulnerable to an XML External Entity attack. If a vulnerable version of the CLI is used to process either a maliciously modified CodeQL database, or a specially prepared set of QL query sources, the CLI can be made to make an outgoing HTTP request to an URL that contains material read from a local file chosen by the attacker. This may result in a loss of privacy of exfiltration of secrets. Security researchers and QL authors who receive databases or QL source files from untrusted sources may be impacted. A single untrusted `.ql` or `.qll` file cannot be affected, but a zip archive or tarball containing QL sources may unpack auxiliary files that will trigger an attack when CodeQL sees them in the file system. Those using CodeQL for routine analysis of source trees with a preselected set of trusted queries are not affected. In particular, extracting XML files from a source tree into the CodeQL database does not make one vulnerable. The problem is fixed in release 2.16.3 of the CodeQL CLI. Other than upgrading, workarounds include not accepting CodeQL databases or queries from untrusted sources, or only processing such material on a machine without an Internet connection. Customers who use older releases of CodeQL for security scanning in an automated CI system and cannot upgrade for compliance reasons can continue using that version. That use case is safe. If such customers have a private query pack and use the `codeql pack create` command to precompile them before using them in the CI system, they should be using the production CodeQL release to run `codeql pack create`. That command is safe as long as the QL source it precompiled is trusted. All other development of the query pack should use an upgraded CLI.	2024-02-22	2.7	CVE-2024-25129

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gitlab -- gitlab	An issue has been discovered in GitLab affecting all versions before 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. It was possible for group members with sub-maintainer role to change the title of privately accessible deploy keys associated with projects in the group.	2024-02-21	3.7	CVE-2023-3509
hcl_software -- hcl_sametime_chat	Sametime Connect desktop chat client includes, but does not use or require, the use of an Eclipse feature called Secure Storage. Using this Eclipse feature to store sensitive data can lead to exposure of that data.	2024-02-23	3.9	CVE-2023-37540
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.7 could allow an authenticated privileged user to obtain the absolute path of the web server installation which could aid in further attacks against the system. IBM X-Force ID: 275777.	2024-02-21	2.4	CVE-2023-50955
ibm -- trusteer_ios_sdk	An undisclosed issue in Trusteer iOS SDK for mobile versions prior to 5.7 and Trusteer Android SDK for mobile versions prior to 5.7 may allow uploading of files. IBM X-Force ID: 238535.	2024-02-17	2.2	CVE-2022-42443
lenovo -- thinksystem_sr670_v2	ThinkSystem SR670V2 servers manufactured from approximately June 2021 to July 2023 were left in Manufacturing Mode which could allow an attacker with privileged logical access to the host or physical access to server internals to modify or disable Intel Boot Guard firmware integrity, SPS security, and other SPS configuration setting. The server's NIST SP 800-193-compliant Platform Firmware Resiliency (PFR) security subsystem significantly mitigates this issue.	2024-02-16	2	CVE-2024-23591 psirt@lenovo.com
linux -- linux	A vulnerability classified as problematic was found in Limbas 5.2.14. Affected by this vulnerability is an unknown functionality of the file main_admin.php. The manipulation of the argument tab_group leads to sql injection. 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-254575. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-23	3.9	CVE-2024-1784
moodle -- moodle	Insufficient checks in a web service made it possible to add comments to the comments block on another user's dashboard when it was not otherwise available (e.g., on their profile page).	2024-02-19	3.5	CVE-2024-25983
nodejs -- undici	Undici is an HTTP/1.1 client, written from scratch for Node.js. Undici already cleared Authorization headers on cross-origin redirects, but did not clear `Proxy-Authentication` headers. This issue has been patched in versions 5.28.3 and 6.6.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-16	3.9	CVE-2024-24758
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 unauthorized read access to a subset of Oracle Audit Vault and Database Firewall accessible data. CVSS 3.1 Base Score 2.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:L/I:N/A:N).	2024-02-17	2.6	CVE-2024-20911
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 network access via multiple protocols 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 read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments,	2024-02-17	3.1	CVE-2024-20923

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).			
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 network access via multiple protocols 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 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 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).	2024-02-17	3.1	CVE-2024-20925
oracle_corporation -- jd_edwards_enterpriseone_tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure SEC). Supported versions that are affected are Prior to 9.2.8.0. 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 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).	2024-02-17	2.7	CVE-2024-20905
phpgurukul -- tourism_management_system	A vulnerability classified as problematic has been found in PHPGurukul Tourism Management System 1.0. Affected is an unknown function of the file user-bookings.php. The manipulation of the argument Full 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-254610 is the identifier assigned to this vulnerability.	2024-02-23	2.4	CVE-2024-1822
renesas -- rcar_gen3_v2.5	During the secure boot, bl2 (the second stage of the bootloader) loops over images defined in the table "bl2_mem_params_descs". For each image, the bl2 reads the image length and destination from the image's certificate. Because of the way of reading from the image, which base on 32-bit unsigned integer value, it can result to an integer overflow. An attacker can bypass memory range restriction and write data out of buffer bounds, which could result in bypass of secure boot. Affected git version from c2f286820471ed276c57e603762bd831873e5a17	2024-02-19	2	CVE-2024-1633 cve@asrg.io
sourcecodester -- simple_student_attendance_system	A vulnerability was found in SourceCodester Simple Student Attendance System 1.0. It has been classified as problematic. This affects an unknown part of the file ?page=attendance&class_id=1. The manipulation of the argument class_date with the input 2024-02-23%22%3E%3Cscript%3Ealert(1)%3C/script%3E 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-254625 was assigned to this vulnerability.	2024-02-23	3.5	CVE-2024-1834
totolink -- x6000r	A vulnerability classified as problematic was found in Totolink X6000R 9.4.0cu.852_B20230719. Affected by this vulnerability is an unknown functionality of the file /etc/shadow. The manipulation leads to hard-coded credentials. It is possible to launch the attack on the local host. 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-	2024-02-20	2.5	CVE-2024-1661

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	254179. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
alfio-event -- alf.io	Alf.io is a free and open-source event attendance management system. An administrator on the alf.io application is able to upload HTML files that trigger JavaScript payloads. As such, an attacker gaining administrative access to the alf.io application may be able to persist access by planting an XSS payload. This issue has been addressed in version 2.0-M4-2402. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-16	3.5	CVE-2024-25627
beyondtrust -- privilege_management_for_windows	Prior to version 24.1, a local authenticated attacker can view Sysvol when Privilege Management for Windows is configured to use a GPO policy. This allows them to view the policy and potentially find configuration issues.	2024-02-16	3.3	CVE-2024-1591 13061848-ea10-403d-bd75-c83a022c2891
dbartholomae -- lambda-middleware_frameguard	A vulnerability, which was classified as problematic, has been found in dbartholomae lambda-middleware frameguard up to 1.0.4. Affected by this issue is some unknown functionality of the file packages/json-deserializer/src/JsonDeserializer.ts of the component JSON Mime-Type Handler. The manipulation leads to inefficient regular expression complexity. Upgrading to version 1.1.0 is able to address this issue. The patch is identified as f689404d830cbc1edd6a1018d3334ff5f44dc6a6. It is recommended to upgrade the affected component. VDB-253406 is the identifier assigned to this vulnerability.	2024-02-12	3.5	CVE-2021-4437
f5 -- big-ip	An SQL injection vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2024-02-14	3.8	CVE-2024-23603
gambio -- gambio	Cleartext Storage of Sensitive Information in Gambio 4.9.2.0 allows attackers to obtain sensitive information via error-handler.log.json and legacy-error-handler.log.txt under the webroot.	2024-02-12	2.7	CVE-2024-23760
ibm -- trusteer_ios_sdk	An undisclosed issue in Trusteer iOS SDK for mobile versions prior to 5.7 and Trusteer Android SDK for mobile versions prior to 5.7 may allow uploading of files. IBM X-Force ID: 238535.	2024-02-17	2.2	CVE-2022-42443
intel -- intel(r)_mas_software	Race condition in some Intel(R) MAS software before version 2.3 may allow a privileged user to potentially enable escalation of privilege via local access.	2024-02-14	1.8	CVE-2023-41090
intel -- intel(r)_sgx_dcap_software_for_windows	Improper input validation in some Intel(R) SGX DCAP software for Windows before version 1.19.100.3 may allow an authenticated user to potentially enable information disclosure via local access.	2024-02-14	3.8	CVE-2023-42776
intel -- intel(r)_thunderbolt(tm)_dch_drivers_for_windows	Deserialization of untrusted data in some Intel(R) Thunderbolt(TM) DCH drivers for Windows before version 88 may allow an authenticated user to potentially enable a denial of service via local access.	2024-02-14	3.8	CVE-2023-26592
intel -- intel(r)_thunderbolt(tm)_dch_drivers_for_windows	Improper buffer restrictions in some Intel(R) Thunderbolt(TM) DCH drivers for Windows before version 88 may allow an authenticated user to potentially enable information disclosure via local access.	2024-02-14	3.8	CVE-2023-27300

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
intel -- intel(r)_thunderbolt(tm)_dch_drivers_for_windows	Improper access control in some Intel(R) Thunderbolt(TM) DCH drivers for Windows before version 88 may allow an authenticated user to potentially enable information disclosure via local access.	2024-02-14	3.8	CVE-2023-27303
intel -- intel(r)_thunderbolt(tm)_dch_drivers_for_windows	Improper buffer restrictions in some Intel(R) Thunderbolt(TM) DCH drivers for Windows before version 88 may allow an authenticated user to potentially enable information disclosure via local access.	2024-02-14	3.8	CVE-2023-27307
intel -- intel(r)_thunderbolt(tm)_dch_drivers_for_windows	Unchecked return value in some Intel(R) Thunderbolt(TM) DCH drivers for Windows before version 88 may allow an unauthenticated user to potentially enable denial of service via physical access.	2024-02-14	2	CVE-2023-26591
intel -- intel(r)_thunderbolt(tm)_dch_drivers_for_windows	Improper access control in some Intel(R) Thunderbolt(TM) DCH drivers for Windows before version 88 may allow an authenticated user to potentially enable denial of service via local access.	2024-02-14	2.5	CVE-2023-26596
kde -- plasma_workspace	A vulnerability, which was classified as problematic, was found in KDE Plasma Workspace up to 5.93.0. This affects the function EventPluginsManager::enabledPlugins of the file components/calendar/eventpluginsmanager.cpp of the component Theme File Handler. The manipulation of the argument pluginId leads to path traversal. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The patch is named 6cdf42916369ebf4ad5bd876c4dfa0170d7b2f01. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-253407. NOTE: This requires write access to user's home or the installation of third party global themes.	2024-02-11	3.1	CVE-2024-1433
lenovo -- thinksystem_sr670_v2	ThinkSystem SR670V2 servers manufactured from approximately June 2021 to July 2023 were left in Manufacturing Mode which could allow an attacker with privileged logical access to the host or physical access to server internals to modify or disable Intel Boot Guard firmware integrity, SPS security, and other SPS configuration setting.	2024-02-16	2	CVE-2024-23591 psirt@lenovo.com
mastodon -- mastodon	Mastodon is a free, open-source social network server based on ActivityPub. When an OAuth Application is destroyed, the streaming server wasn't being informed that the Access Tokens had also been destroyed, this could have posed security risks to users by allowing an application to continue listening to streaming after the application had been destroyed. Essentially this comes down to the fact that when Doorkeeper sets up the relationship between Applications and Access Tokens, it uses a `dependent: delete_all` configuration, which means the `after_commit` callback setup on `AccessTokenExtension` didn't actually fire, since `delete_all` doesn't trigger ActiveRecord callbacks. To mitigate, we need to add a `before_destroy` callback to `ApplicationExtension` which announces to streaming that all the Application's Access Tokens are being "killed". Impact should be negligible given the affected application had to be owned by the user. None the less this issue has been addressed in versions 4.2.6, 4.1.14, 4.0.14, and 3.5.18. Users are advised to upgrade. There is no known workaround for this vulnerability.	2024-02-14	3.1	CVE-2024-25619
mattermost -- mattermost_server	Mattermost Jira Plugin fails to protect against logout CSRF allowing an attacker to post a specially crafted message that would disconnect a user's Jira connection in Mattermost only by viewing the message.	2024-02-09	3.5	CVE-2024-23319

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nodejs -- undici	Undici is an HTTP/1.1 client, written from scratch for Node.js. Undici already cleared Authorization headers on cross-origin redirects but did not clear `Proxy-Authentication` headers. This issue has been patched in versions 5.28.3 and 6.6.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-02-16	3.9	CVE-2024-24758
opensc -- authentic_driver	The use-after-free vulnerability was found in the AuthentIC driver in OpenSC packages, occurring in the card enrolment process using pkcs15-init when a user or administrator enrolls or modifies cards. An attacker must have physical access to the computer system and requires a crafted USB device or smart card to present the system with specially crafted responses to the APDUs, which are considered high complexity and low severity. This manipulation can allow for compromised card management operations during enrolment.	2024-02-12	3.4	CVE-2024-1454
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 unauthorized read access to a subset of Oracle Audit Vault and Database Firewall accessible data. CVSS 3.1 Base Score 2.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:L/I:N/A:N).	2024-02-17	2.6	CVE-2024-20911
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 network access via multiple protocols 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 read access to a subset 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 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 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).	2024-02-17	3.1	CVE-2024-20923
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 network access via multiple protocols 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 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 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).	2024-02-17	3.1	CVE-2024-20925
oracle_corporation -- jd_edwards_enter	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure SEC). Supported versions that are affected are Prior to 9.2.8.0. Easily exploitable vulnerability allows high privileged attacker with network access via JDENET to compromise JD Edwards EnterpriseOne Tools.	2024-02-17	2.7	CVE-2024-20905

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
priseone_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 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).			
sametime -- sametime	Sametime is impacted by a failure to invalidate sessions. The application is setting sensitive cookie values in a persistent manner in Sametime Web clients. When this happens, cookie values can remain valid even after a user has closed out their session.	2024-02-09	3.9	CVE-2023-45718
sametime -- sametime	Sametime is impacted by sensitive information passed in URL.	2024-02-09	1.7	CVE-2023-45716
siemens -- parasolid_v35.0	A vulnerability has been identified in Parasolid V35.0 (All versions < V35.0.251), Parasolid V35.1 (All versions < V35.1.170). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted XT files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	2024-02-13	3.3	CVE-2024-22043
armcode -- alienip	A vulnerability classified as problematic has been found in Armcode AlienIP 2.41. Affected is an unknown function of the component Locate Host Handler. The manipulation leads to denial of service. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252684. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-02	3.3	CVE-2024-1194
codeastro -- restaurant_pos_system	A vulnerability, which was classified as problematic, has been found in CodeAstro Restaurant POS System 1.0. Affected by this issue is some unknown functionality of the file create_account.php. The manipulation of the argument Full Name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-253010 is the identifier assigned to this vulnerability.	2024-02-07	3.5	CVE-2024-1267
codeastro -- university_management_system	A vulnerability classified as problematic has been found in CodeAstro University Management System 1.0. Affected is an unknown function of the file /att_add.php of the component Attendance Management. The manipulation of the argument Student 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-253008.	2024-02-07	2.4	CVE-2024-1265
codeastro -- university_management_system	A vulnerability classified as problematic was found in CodeAstro University Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /st_reg.php of the component Student Registration Form. The manipulation of the argument Address 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-253009 was assigned to this vulnerability.	2024-02-07	2.4	CVE-2024-1266
concrete_cms -- concrete_cms	Concrete CMS version 9 before 9.2.5 is vulnerable to stored XSS in file tags and description attributes since administrator entered file attributes are not sufficiently sanitized in the Edit Attributes page. A rogue administrator could put malicious code into the file tags or description attributes and, when another administrator opens the same file for editing, the malicious code could execute. The Concrete CMS Security team scored this 2.4 with CVSS v3 vector AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N.	2024-02-09	2.4	CVE-2024-1245
concrete_cms -- concrete_cms	Concrete CMS in version 9 before 9.2.5 is vulnerable to reflected XSS via the Image URL Import Feature due to insufficient validation of administrator provided data. A rogue administrator could inject malicious code when importing images, leading to the execution of the malicious code on the website user's browser. The Concrete CMS Security team scored this 2 with CVSS v3 vector	2024-02-09	2	CVE-2024-1246

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N. This does not affect Concrete versions prior to version 9.			
concrete_cms -- concrete_cms	Concrete CMS version 9 before 9.2.5 is vulnerable to stored XSS via the Role Name field since there is insufficient validation of administrator provided data for that field. A rogue administrator could inject malicious code into the Role Name field which might be executed when users visit the affected page. The Concrete CMS Security team scored this 2 with CVSS v3 vector AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator . Concrete versions below 9 do not include group types so they are not affected by this vulnerability.	2024-02-09	2	CVE-2024-1247
grub2 -- grub2	A flaw was found in the grub2-set-bootflag utility of grub2. After the fix of CVE-2019-14865, grub2-set-bootflag will create a temporary file with the new grubenv content and rename it to the original grubenv file. If the program is killed before the rename operation, the temporary file will not be removed and may fill the filesystem when invoked multiple times, resulting in a filesystem out of free inodes or blocks.	2024-02-06	3.3	CVE-2024-1048
hcl_software -- hcl_sametime	Sametime is impacted by a failure to invalidate sessions. The application is setting sensitive cookie values in a persistent manner in Sametime Web clients. When this happens, cookie values can remain valid even after a user has closed out their session.	2024-02-09	3.9	CVE-2023-45718
juanpao -- jpshop	A vulnerability was found in Juanpao JPShop up to 1.5.02. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file api/config/params.php of the component API. The manipulation of the argument JWT_KEY_ADMIN leads to use of hard-coded cryptographic key . 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-252997 was assigned to this vulnerability.	2024-02-06	3.1	CVE-2024-1258
mailcow -- mailcow-dockerized	mailcow is a dockerized email package, with multiple containers linked in one bridged network. The application is vulnerable to pixel flood attack, once the payload has been successfully uploaded in the logo the application goes slow and doesn't respond in the admin page. It is tested on the versions 2023-12a and prior and patched in version 2024-01.	2024-02-02	2.7	CVE-2024-23824
mattermost -- mattermost	Mattermost Jira Plugin fails to protect against logout CSRF allowing an attacker to post a specially crafted message that would disconnect a user's Jira connection in Mattermost only by viewing the message.	2024-02-09	3.5	CVE-2024-23319
mattermost -- mattermost	Mattermost Jira Plugin handling subscriptions fails to check the security level of an incoming issue or limit it based on the user who created the subscription resulting in registered users on Jira being able to create webhooks that give them access to all Jira issues.	2024-02-09	3.4	CVE-2024-24774
mattermost -- mattermost	Mattermost fails to check the required permissions in the POST /api/v4/channels/stats/member_count API resulting in channel member counts being leaked to a user without permissions.	2024-02-09	3.1	CVE-2024-24776
planet-freo -- planet-freo	A vulnerability was found in planet-freo up to 20150116 and classified as problematic. Affected by this issue is some unknown functionality of the file admin/inc/auth.inc.php. The manipulation of the argument auth leads to incorrect comparison. 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. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The name of the patch is 6ad38c58a45642eb8c7844e2f272ef199f59550d. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-252716.	2024-02-04	3.7	CVE-2015-10129

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sametime -- sametime	Sametime is impacted by sensitive information passed in URL.	2024-02-09	1.7	CVE-2023-45716
samsung_mobile -- samsung_internet	Improper authorization verification vulnerability in Samsung Internet prior to version 24.0 allows physical attackers to access files downloaded in SecretMode without proper authentication.	2024-02-06	2.4	CVE-2024-20828
samsung_mobile -- samsung_mobile_devices	Implicit intent hijacking vulnerability in Smart Suggestions prior to SMR Feb-2024 Release 1 allows attackers to get sensitive information.	2024-02-06	3.3	CVE-2024-20810
sourcecodester -- crud	A vulnerability was found in SourceCodester CRUD without Page Reload 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file fetch_data.php. The manipulation of the argument username/city leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-252782 is the identifier assigned to this vulnerability.	2024-02-03	3.5	CVE-2024-1215
sourcecodester -- product_management_system	A vulnerability has been found in SourceCodester Product Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /supplier.php. The manipulation of the argument supplier_name/supplier_contact leads to cross site scripting. 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-253012.	2024-02-07	2.4	CVE-2024-1269
sulu-- sulu	Sulu is a highly extensible open-source PHP content management system based on the Symfony framework. There is an issue when inputting HTML into the Tag name. The HTML is executed when the tag name is listed in the auto complete form. Only admin users can create tags so they are the only ones affected. The problem is patched with version(s) 2.4.16 and 2.5.12.	2024-02-05	2.7	CVE-2024-24807
vyperlang -- vyper	Vyper is a Pythonic Smart Contract Language for the EVM. There is an error in the stack management when compiling the `IR` for `sha3_64`. Concretely, the `height` variable is miscalculated. The vulnerability can't be triggered without writing the `IR` by hand (that is, it cannot be triggered from regular vyper code). `sha3_64` is used for retrieval in mappings. No flow that would cache the `key` was found so the issue shouldn't be possible to trigger when compiling the compiler-generated `IR`. This issue isn't triggered during normal compilation of vyper code so the impact is low. At the time of publication there is no patch available.	2024-02-05	3.7	CVE-2024-24559
vyperlang -- vyper	Vyper is a Pythonic Smart Contract Language for the Ethereum Virtual Machine. When calls to external contracts are made, we write the input buffer starting at byte 28, and allocate the return buffer to start at byte 0 (overlapping with the input buffer). When checking RETURNDATASIZE for dynamic types, the size is compared only to the minimum allowed size for that type, and not to the returned value's length. As a result, malformed return data can cause the contract to mistake data from the input buffer for returndata. When the called contract returns invalid ABIv2 encoded data, the calling contract can read different invalid data (from the dirty buffer) than the called contract returned.	2024-02-02	3.7	CVE-2024-24560
wordpress -- wordpress	The WP RSS Aggregator plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 4.23.5 via the RSS feed source in admin settings. This makes it possible for authenticated attackers, with administrator-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	2024-02-07	3.8	CVE-2024-0628
wordpress -- wordpress	The Minimal Coming Soon - Coming Soon Page plugin for WordPress is vulnerable to maintenance mode bypass and information disclosure in all versions up to, and including, 2.37. This is due to the plugin improperly validating the request path.	2024-02-05	3.7	CVE-2024-1075

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	This makes it possible for unauthenticated attackers to bypass maintenance mode and view pages that should be hidden.			