BULLETIN (SB24-183)

VULNERABILITY SUMMARY FOR THE WEEK OF

24TH JUNE, 2024

Bulletin (SB24-183)
Vulnerability Summary for the Week of June 24, 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
8theme--XStore Core	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in 8theme XStore Core allows PHP Local File Inclusion.This issue affects XStore Core: from n/a through 5.3.8.	2024-06-04	8.5	CVE-2024-33557
8theme--XStore	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in 8theme XStore allows PHP Local File Inclusion.This issue affects XStore: from n/a through 9.3.8.	2024-06-04	9	CVE-2024-33560
ABB, Busch-Jaeger--2.4! Display 55, SD/U12.55.11-825	FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System	2024-06-05	9.6	CVE-2024-4008
ABB, Busch-Jaeger--2.4! Display 55, SD/U12.55.11-825	Replay Attack in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay KNX telegram to local KNX Bus-System	2024-06-05	9.2	CVE-2024-4009
BdThemes--Element Pack Pro	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Deserialization of Untrusted Data vulnerability in BdThemes Element Pack Pro allows Path Traversal, Object Injection.This issue affects Element Pack Pro: from n/a through 7.7.4.	2024-06-04	8.5	CVE-2024-33568
BestWebSoft--Contact Form to DB by BestWebSoft	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in BestWebSoft Contact Form to DB by BestWebSoft.This issue affects Contact Form to DB by BestWebSoft: from n/a through 1.7.2.	2024-06-08	8.5	CVE-2024-35678
Bitdefender--GravityZone Console On-Premise	A host whitelist parser issue in the proxy service implemented in the GravityZone Update Server allows an attacker to cause a server-side request forgery. This issue only affects GravityZone Console versions before 6.38.1-2 that are running only on premise.	2024-06-06	8.1	CVE-2024-4177
bobbysmith007--WP-DB-Table-Editor	The WP-DB-Table-Editor plugin for WordPress is vulnerable to unauthorized access of data, modification of data, and loss of data due to lack of a default capability requirement on the 'dbte_render' function in all versions up to, and including, 1.8.4. This makes it possible for authenticated attackers, with contributor access and above, to modify database tables that the theme has been configured to use the plugin to edit.	2024-06-04	7.5	CVE-2024-2019
chainguard-dev--apko	apko is an apk-based OCI image builder. apko exposures HTTP basic auth credentials from repository and keyring URLs in log output. This vulnerability is fixed in v0.14.5.	2024-06-03	7.5	CVE-2024-36127
Chanjet--Smooth T+system	A vulnerability, which was classified as critical, has been found in Chanjet Smooth T+system 3.5. This issue affects some unknown processing of the file /tplus/UFAQD/keyEdit.aspx. The manipulation of the argument KeyID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-267185 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-05	7.3	CVE-2024-5653
chrisbadgett--LifterLMS WordPress LMS for eLearning	The LifterLMS - WordPress LMS Plugin for eLearning plugin for WordPress is vulnerable to SQL Injection via the orderBy attribute of the lifterlms_favorites shortcode in all versions up to, and including, 7.6.2 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.	2024-06-05	9.8	CVE-2024-4743
Cisco--Cisco Unified Contact Center Enterprise	A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct an SSRF attack on an affected system. This vulnerability is due to insufficient validation of user-supplied input for specific HTTP requests that are sent to an affected system. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to obtain limited sensitive information for services that are associated to the affected device.	2024-06-05	7.2	CVE-2024-20404
Code for Recovery--12 Step Meeting List	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Code for Recovery 12 Step Meeting List allows Reflected XSS.This issue affects 12 Step Meeting List: from n/a through 3.14.33.	2024-06-08	7.1	CVE-2024-35693
Code Parrots--Easy Forms for	Insertion of Sensitive Information into Log File vulnerability in Code Parrots Easy Forms for Mailchimp.This issue affects Easy Forms for Mailchimp: from n/a through 6.9.0.	2024-06-04	7.5	CVE-2024-25095

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Mailchimp				
Codeer Limited--Bricks Builder	Improper Control of Generation of Code ('Code Injection') vulnerability in Codeer Limited Bricks Builder allows Code Injection.This issue affects Bricks Builder: from n/a through 1.9.6.	2024-06-04	10	CVE-2024-25600
codelessthemes--Cowidgets Elementor Addons	The Cowidgets - Elementor Addons plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.1.1 via the 'item_style' and 'style' parameters. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files 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.	2024-06-06	8.8	CVE-2024-5179
CodePeople--WP Time Slots Booking Form	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CodePeople WP Time Slots Booking Form allows Stored XSS.This issue affects WP Time Slots Booking Form: from n/a through 1.2.10.	2024-06-08	7.1	CVE-2024-35734
CODESYS--CODESYS Control for BeagleBone SL	An unauthenticated remote attacker can use a malicious OPC UA client to send a crafted request to affected CODESYS products which can cause a DoS due to incorrect calculation of buffer size.	2024-06-04	7.5	CVE-2024-5000
CODESYS--CODESYS Control Win (SL)	A local attacker with low privileges can read and modify any users files and cause a DoS in the working directory of the affected products due to exposure of resource to wrong sphere.	2024-06-04	7.8	CVE-2023-5751
Dell--CPG BIOS	Dell BIOS contains a missing support for integrity check vulnerability. An attacker with physical access to the system could potentially bypass security mechanisms to run arbitrary code on the system.	2024-06-07	7.6	CVE-2023-32475
Dell--PowerScale OneFS	Dell PowerScale OneFS versions 8.2.x through 9.8.0.x contain a use of hard coded credentials vulnerability. An adjacent network unauthenticated attacker could potentially exploit this vulnerability, leading to information disclosure of network traffic and denial of service.	2024-06-04	8.1	CVE-2024-29170
denoland--deno	An issue in `.npmrc` support in Deno 1.44.0 was discovered where Deno would send `.npmrc` credentials for the scope to the tarball URL when the registry provided URLs for a tarball on a different domain. All users relying on .npmrc are potentially affected by this vulnerability if their private registry references tarball URLs at a different domain. This includes usage of deno install subcommand, auto-install for npm: specifiers and LSP usage. It is recommended to upgrade to Deno 1.44.1 and if your private registry ever serves tarballs at a different domain to rotate your registry credentials.	2024-06-06	7.6	CVE-2024-37150
dexta--Dextaz Ping	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in dexta Dextaz Ping allows Command Injection.This issue affects Dextaz Ping: from n/a through 0.65.	2024-06-04	9.1	CVE-2024-34792
DigiWin--EasyFlow .NET	DigiWin EasyFlow .NET lacks validation for certain input parameters. An unauthenticated remote attacker can inject arbitrary SQL commands to read, modify, and delete database records.	2024-06-03	9.8	CVE-2024-5311
directus--directus	Directus is a real-time API and App dashboard for managing SQL database content. Prior to 10.11.2, providing a non-numeric length value to the random string generation utility will create a memory issue breaking the capability to generate random strings platform wide. This creates a denial of service situation where logged in sessions can no longer be refreshed as sessions depend on the capability to generate a random session ID. This vulnerability is fixed in 10.11.2.	2024-06-03	7.5	CVE-2024-36128
envoyproxy--envoy	Envoy is a cloud-native, open source edge and service proxy. Envoyproxy with a Brotli filter can get into an endless loop during decompression of Brotli data with extra input.	2024-06-04	7.5	CVE-2024-32976
envoyproxy--envoy	Envoy is a cloud-native, open source edge and service proxy. Due to how Envoy invoked the nlohmann JSON library, the library could throw an uncaught exception from downstream data if incomplete UTF-8 strings were serialized. The uncaught exception would cause Envoy to crash.	2024-06-04	7.5	CVE-2024-34363
evmos--evmos	Evmos is the Ethereum Virtual Machine (EVM) Hub on the Cosmos Network. There is an issue with how to liquid stake using Safe which itself is a contract. The bug only appears when there is a local state change together with an ICS20 transfer in the same function and uses the contract's balance, that is using the contract address as the sender parameter in an ICS20 transfer using the ICS20 precompile.	2024-06-06	7.5	CVE-2024-37153

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	This is in essence the "infinite money glitch" allowing contracts to double the supply of Evmos after each transaction.The issue has been patched in versions >=V18.1.0.			
expresstech--Quiz and Survey Master (QSM) Easy Quiz and Survey Maker	The Quiz And Survey Master - Best Quiz, Exam and Survey Plugin for WordPress plugin for WordPress is vulnerable to SQL Injection via the 'question_id' parameter in all versions up to, and including, 9.0.1 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 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.	2024-06-07	9.9	CVE-2024-3592
Fahad Mahmood--WP Docs	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Fahad Mahmood WP Docs allows Reflected XSS.This issue affects WP Docs: from n/a through 2.1.3.	2024-06-08	7.1	CVE-2024-35696
Foliovision--FV Flowplayer Video Player	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Foliovision FV Flowplayer Video Player allows Reflected XSS.This issue affects FV Flowplayer Video Player: from n/a through 7.5.45.7212.	2024-06-03	7.1	CVE-2024-35631
Fortinet--FortiWebManager	An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and 6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI.	2024-06-03	8.8	CVE-2024-23668
Fortinet--FortiWebManager	An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and 6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI.	2024-06-03	7.8	CVE-2024-23667
Fortinet--FortiWebManager	An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and 6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI.	2024-06-03	7.8	CVE-2024-23670
gelform--Social Link Pages: link-in-bio landing pages for your social media profiles	The Social Link Pages: link-in-bio landing pages for your social media profiles plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the import_link_pages() function in all versions up to, and including, 1.6.9. This makes it possible for unauthenticated attackers to inject arbitrary pages and malicious web scripts.	2024-06-04	7.2	CVE-2024-3555
GiveWP--GiveWP	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in GiveWP allows Reflected XSS.This issue affects GiveWP: from n/a through 3.12.0.	2024-06-08	7.1	CVE-2024-35679
Grafana--OnCall	Grafana OnCall is an easy-to-use on-call management tool that will help reduce toil in on-call management through simpler workflows and interfaces that are tailored specifically for engineers. Grafana OnCall, from version 1.1.37 before 1.5.2 are vulnerable to a Server Side Request Forgery (SSRF) vulnerability in the webhook functionallity. This issue was fixed in version 1.5.2	2024-06-05	7.7	CVE-2024-5526 security@grafana.com
HCL Software--Domino Server	The Domino Catalog template is susceptible to a Stored Cross-Site Scripting (XSS) vulnerability. An attacker with the ability to edit documents in the catalog application/database created from this template can embed a cross site scripting attack. The attack would be activated by an end user clicking it.	2024-06-06	8.4	CVE-2023-37539
IBM--Engineering Requirements Management DOORS Next	IBM Engineering Requirements Management DOORS Next 7.0.2 and 7.0.3 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: 268758.	2024-06-06	8.2	CVE-2023-45192
icegram--Email Subscribers by Icegram Express Email Marketing, Newsletters, Automation for WordPress & WooCommerce	The Email Subscribers by Icegram Express plugin for WordPress is vulnerable to SQL Injection via the 'hash' parameter in all versions up to, and including, 5.7.20 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.	2024-06-05	9.8	CVE-2024-4295
idccms -- idccms	idccms V1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component admin/vpsClass_deal.php?mudi=add	2024-06-04	8.8	CVE-2024-36547
idccms -- idccms	idccms V1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via admin/vpsCompany_deal.php?mudi=del	2024-06-04	8.8	CVE-2024-36548
idccms -- idccms	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via /admin/vpsCompany_deal.php?mudi=rev&nohrefStr=close	2024-06-04	8.8	CVE-2024-36549

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
idccms -- idccms	idccms V1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via /admin/vpsCompany_deal.php?mudi=add&nohrefStr=close	2024-06-04	8.8	CVE-2024-36550
ifm--moneo appliance QVA200	An unauthenticated remote attacker can change the admin password in a moneo appliance due to weak password recovery mechanism.	2024-06-03	9.8	CVE-2024-5404
itsourcecode--Bakery Online Ordering System	A vulnerability was found in itsourcecode Bakery Online Ordering System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/modules/product/controller.php?action=add. The manipulation of the argument image 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-267414 is the identifier assigned to this vulnerability.	2024-06-07	7.3	CVE-2024-5745
itsourcecode--Online Discussion Forum	A vulnerability was found in itsourcecode Online Discussion Forum 1.0. It has been rated as critical. This issue affects some unknown processing of the file register_me.php. The manipulation of the argument eaddress leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-267407.	2024-06-07	7.3	CVE-2024-5733
jupyter-server--jupyter_server	The Jupyter Server provides the backend for Jupyter web applications. Jupyter Server on Windows has a vulnerability that lets unauthenticated attackers leak the NTLMv2 password hash of the Windows user running the Jupyter server. An attacker can crack this password to gain access to the Windows machine hosting the Jupyter server, or access other network-accessible machines or 3rd party services using that credential. Or an attacker perform an NTLM relay attack without cracking the credential to gain access to other network-accessible machines. This vulnerability is fixed in 2.14.1.	2024-06-06	7.5	CVE-2024-35178
kanboard--kanboard	Kanboard is project management software that focuses on the Kanban methodology. The vuln is in app/Controller/ProjectPermissionController.php function addUser(). The users permission to add users to a project only get checked on the URL parameter project_id. If the user is authorized to add users to this project the request gets processed. The users permission for the POST BODY parameter project_id does not get checked again while processing. An attacker with the 'Project Manager' on a single project may take over any other project. The vulnerability is fixed in 1.2.37.	2024-06-06	8.2	CVE-2024-36399
litonice13--Master Addons Free Widgets, Hover Effects, Toggle, Conditions, Animations for Elementor	The Master Addons - Free Widgets, Hover Effects, Toggle, Conditions, Animations for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Navigation Menu widget of the plugin's Mega Menu extension in all versions up to, and including, 2.0.6.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-07	7.2	CVE-2024-5542
LJ Apps--WP TripAdvisor Review Slider	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LJ Apps WP TripAdvisor Review Slider allows Blind SQL Injection.This issue affects WP TripAdvisor Review Slider: from n/a through 12.6.	2024-06-03	7.6	CVE-2024-35630
Loopus--WP Visitors Tracker	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Loopus WP Visitors Tracker allows Reflected XSS.This issue affects WP Visitors Tracker: from n/a through 2.3.	2024-06-08	7.1	CVE-2024-35737
lvaudore--The Moneytizer	The The Moneytizer plugin for WordPress is vulnerable to unauthorized access of data, modification of data, and loss of data due to a missing capability check on multiple AJAX functions in the /core/core_ajax.php file in all versions up to, and including, 9.5.20. This makes it possible for authenticated attackers, with subscriber access and above, to update and retrieve billing and bank details, update and reset the plugin's settings, and update languages as well as other lower-severity actions.	2024-06-06	8.1	CVE-2023-6966
lvaudore--The Moneytizer	The The Moneytizer plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 9.5.20. This is due to missing or incorrect nonce validation on multiple AJAX functions. This makes it possible for unauthenticated attackers to to update and retrieve billing and bank details, update and reset the plugin's settings, and update languages as well as other lower-severity actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-06-06	8.1	CVE-2023-6968
misskey-dev--misskey	Misskey is an open source, decentralized microblogging platform. Misskey doesn't perform proper normalization on the JSON structures of incoming signed ActivityPub activity objects before processing them, allowing threat actors to spoof	2024-06-03	8.2	CVE-2024-32983

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the contents of signed activities and impersonate the authors of the original activities. This vulnerability is fixed in 2024.5.0.			
MLflow--MLflow	Deserialization of untrusted data can occur in versions of the MLflow platform running version 1.1.0 or newer, enabling a maliciously uploaded scikit-learn model to run arbitrary code on an end user's system when interacted with.	2024-06-04	8.8	CVE-2024-37052
MLflow--MLflow	Deserialization of untrusted data can occur in versions of the MLflow platform running version 1.1.0 or newer, enabling a maliciously uploaded scikit-learn model to run arbitrary code on an end user's system when interacted with.	2024-06-04	8.8	CVE-2024-37053
MLflow--MLflow	Deserialization of untrusted data can occur in versions of the MLflow platform running version 0.9.0 or newer, enabling a maliciously uploaded PyFunc model to run arbitrary code on an end user's system when interacted with.	2024-06-04	8.8	CVE-2024-37054
MLflow--MLflow	Deserialization of untrusted data can occur in versions of the MLflow platform running version 1.24.0 or newer, enabling a maliciously uploaded pmdarima model to run arbitrary code on an end user's system when interacted with.	2024-06-04	8.8	CVE-2024-37055
MLflow--MLflow	Deserialization of untrusted data can occur in versions of the MLflow platform running version 1.23.0 or newer, enabling a maliciously uploaded LightGBM scikit-learn model to run arbitrary code on an end user's system when interacted with.	2024-06-04	8.8	CVE-2024-37056
MLflow--MLflow	Deserialization of untrusted data can occur in versions of the MLflow platform running version 2.0.0rc0 or newer, enabling a maliciously uploaded Tensorflow model to run arbitrary code on an end user's system when interacted with.	2024-06-04	8.8	CVE-2024-37057
MLflow--MLflow	Deserialization of untrusted data can occur in versions of the MLflow platform running version 2.5.0 or newer, enabling a maliciously uploaded Langchain AgentExecutor model to run arbitrary code on an end user's system when interacted with.	2024-06-04	8.8	CVE-2024-37058
MLflow--MLflow	Deserialization of untrusted data can occur in versions of the MLflow platform running version 0.5.0 or newer, enabling a maliciously uploaded PyTorch model to run arbitrary code on an end user's system when interacted with.	2024-06-04	8.8	CVE-2024-37059
MLflow--MLflow	Deserialization of untrusted data can occur in versions of the MLflow platform running version 1.27.0 or newer, enabling a maliciously crafted Recipe to execute arbitrary code on an end user's system when run.	2024-06-04	8.8	CVE-2024-37060
MLflow--MLflow	Remote Code Execution can occur in versions of the MLflow platform running version 1.11.0 or newer, enabling a maliciously crafted MLproject to execute arbitrary code on an end user's system when run.	2024-06-04	8.8	CVE-2024-37061
n/a--Clash	A vulnerability was found in Clash up to 0.20.1 on Windows. It has been declared as critical. This vulnerability affects unknown code of the component Proxy Port. The manipulation leads to improper authentication. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to change the configuration settings. VDB-267406 is the identifier assigned to this vulnerability.	2024-06-07	7.3	CVE-2024-5732
n/a--n/a	An issue was discovered in Samsung Mobile Processor Exynos 2200, Exynos 1480, Exynos 2400. It lacks a check for the validation of native handles, which can result in code execution.	2024-06-07	8.4	CVE-2024-31959
n/a--n/a	An issue was discovered in Samsung Mobile Processor and Wearable Processor Exynos 850, Exynos 1080, Exynos 2100, Exynos 1280, Exynos 1380, Exynos 1330, Exynos W920, Exynos W930. The mobile processor lacks proper reference count checking, which can result in a UAF (Use-After-Free) vulnerability.	2024-06-07	8.4	CVE-2024-32502
n/a--n/a	An issue was discovered in Samsung Mobile Processor and Wearable Processor Exynos 850, Exynos 1080, Exynos 2100, Exynos 1280, Exynos 1380, Exynos 1330, Exynos W920, Exynos W930. The mobile processor lacks proper memory deallocation checking, which can result in a UAF (Use-After-Free) vulnerability.	2024-06-07	8.4	CVE-2024-32503
Netgsm--Netgsm	Missing Authorization vulnerability in Netgsm.This issue affects Netgsm: from n/a through 2.9.16.	2024-06-04	7.5	CVE-2024-35672
open-telemetry--opentelemetry-collector	The OpenTelemetry Collector offers a vendor-agnostic implementation on how to receive, process and export telemetry data. An unsafe decompression vulnerability allows unauthenticated attackers to crash the collector via excessive memory consumption. OTel Collector version 0.102.1 fixes this issue. It is also fixed in the confighttp module version 0.102.0 and configgrpc module version 0.102.1.	2024-06-05	8.2	CVE-2024-36129
phoeniixx--Social Login Lite For WooCommerce	The Social Login Lite For WooCommerce plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 1.6.0. This is due to insufficient verification on the user being supplied during the social login through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email.	2024-06-04	9.8	CVE-2024-4552
pimcore--pimcore	Pimcore is an Open Source Data & Experience Management Platform. The Pimcore thumbnail generation can be used to flood the server with large files. By changing the file extension or scaling factor of the requested thumbnail, attackers can create	2024-06-04	7.5	CVE-2024-32871

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	files that are much larger in file size than the original. This vulnerability is fixed in 11.2.4.			
pokornydavid--Frontend Registration Contact Form 7	The Frontend Registration - Contact Form 7 plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 5.1 due to insufficient restriction on the '_cf7frr_' post meta. This makes it possible for authenticated attackers, with editor-level access and above, to modify the default user role in the registration form settings.	2024-06-04	7.2	CVE-2024-4870
PORTY Smart Tech Technology Joint Stock Company--PowerBank Application	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in PORTY Smart Tech Technology Joint Stock Company PowerBank Application allows Retrieve Embedded Sensitive Data.This issue affects PowerBank Application: before 2.02.	2024-06-05	7.2	CVE-2024-1662
PowerPack--PowerPack Pro for Elementor	The PowerPack Pro for Elementor plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 2.10.17. This is due to the plugin not restricting low privileged users from setting a default role for a registration form. This makes it possible for authenticated attackers, with contributor-level access and above, to create a registration form with administrator set as the default role and then register as an administrator.	2024-06-08	8.8	CVE-2024-3668
qodeinteractive--Qi Addons For Elementor	The Qi Addons For Elementor plugin for WordPress is vulnerable to Remote File Inclusion in all versions up to, and including, 1.7.2 via the 'behavior' attributes found in the qi_addons_for_elementor_blog_list shortcode. This makes it possible for authenticated attackers, with Contributor-level access and above, to include remote files on the server, resulting in code execution. Please note that this requires an attacker to create a non-existent directory or target an instance where file_exists won't return false with a non-existent directory in the path, in order to successfully exploit.	2024-06-07	7.5	CVE-2024-4887
Qualcomm, Inc.--Snapdragon	Memory corruption in TZ Secure OS while Tunnel Invoke Manager initialization.	2024-06-03	9.3	CVE-2023-43538
Qualcomm, Inc.--Snapdragon	Cryptographic issue while performing attach with a LTE network, a rogue base station can skip the authentication phase and immediately send the Security Mode Command.	2024-06-03	9.1	CVE-2023-43551
Qualcomm, Inc.--Snapdragon	Memory corruption in Hypervisor when platform information mentioned is not aligned.	2024-06-03	9.3	CVE-2023-43556
Qualcomm, Inc.--Snapdragon	Information disclosure in Video while parsing mp2 clip with invalid section length.	2024-06-03	8.2	CVE-2023-43555
Qualcomm, Inc.--Snapdragon	Memory corruption while creating a LPAC client as LPAC engine was allowed to access GPU registers.	2024-06-03	8.4	CVE-2024-23360
Qualcomm, Inc.--Snapdragon	Memory corruption while copying a keyblob`s material when the key material`s size is not accurately checked.	2024-06-03	7.8	CVE-2023-43542
Qualcomm, Inc.--Snapdragon	Transient DOS while processing an improperly formatted Fine Time Measurement (FTM) management frame.	2024-06-03	7.5	CVE-2024-23363
realmag777--Active Products Tables for WooCommerce	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in realmag777 Active Products Tables for WooCommerce allows Reflected XSS.This issue affects Active Products Tables for WooCommerce: from n/a through 1.0.6.3.	2024-06-08	7.1	CVE-2024-35730
Red Hat--Logging Subsystem for Red Hat OpenShift	A flaw was found in OpenShift's Telemeter. If certain conditions are in place, an attacker can use a forged token to bypass the issue ("iss") check during JSON web token (JWT) authentication.	2024-06-05	7.5	CVE-2024-5037
Red Hat--Red Hat Build of Keycloak	A flaw was found in Keycloak in OAuth 2.0 Pushed Authorization Requests (PAR). Client-provided parameters were found to be included in plain text in the KC_RESTART cookie returned by the authorization server's HTTP response to a `request_uri` authorization request, possibly leading to an information disclosure vulnerability.	2024-06-03	7.5	CVE-2024-4540

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--Red Hat Enterprise Linux 8	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server.	2024-06-06	7.4	CVE-2024-3049
Repute Infosystems--ARMember	Improper Privilege Management vulnerability in Repute Infosystems ARMember allows Privilege Escalation.This issue affects ARMember: from n/a through 4.0.10.	2024-06-04	8.3	CVE-2023-47837
RLDD--Auto Coupons for WooCommerce	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in RLDD Auto Coupons for WooCommerce allows Reflected XSS.This issue affects Auto Coupons for WooCommerce: from n/a through 3.0.14.	2024-06-08	7.1	CVE-2024-35733
Samsung Mobile--Samsung Mobile Devices	Improper access control vulnerability in SmartManagerCN prior to SMR Jun-2024 Release 1 allows local attackers to launch privileged activities.	2024-06-04	7.9	CVE-2024-20874
Samsung Mobile--Samsung Mobile Devices	Heap out-of-bound write vulnerability in parsing grid image header in libsavscmn.so prior to SMR Jun-2024 Release 1 allows local attackers to execute arbitrary code.	2024-06-04	7.3	CVE-2024-20877
Samsung Mobile--Samsung Mobile Devices	Heap out-of-bound write vulnerability in parsing grid image in libsavscmn.so prior to SMR June-2024 Release 1 allows local attackers to execute arbitrary code.	2024-06-04	7.3	CVE-2024-20878
Select-Themes--Stockholm Core	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Select-Themes Stockholm Core allows PHP Local File Inclusion.This issue affects Stockholm Core: from n/a through 2.4.1.	2024-06-04	8.5	CVE-2024-34554
Select-Themes--Stockholm	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Select-Themes Stockholm allows PHP Local File Inclusion.This issue affects Stockholm: from n/a through 9.6.	2024-06-04	9	CVE-2024-34551
Select-Themes--Stockholm	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Select-Themes Stockholm allows PHP Local File Inclusion.This issue affects Stockholm: from n/a through 9.6.	2024-06-04	8.5	CVE-2024-34552
Skops-dev--Skops	Deserialization of untrusted data can occur in versions 0.6 or newer of the skops python library, enabling a maliciously crafted model to run arbitrary code on an end user's system when loaded.	2024-06-04	7.8	CVE-2024-37065
softaculous--FileOrganizer Manage WordPress and Website Files	The FileOrganizer - Manage WordPress and Website Files plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.0.7 via the 'fileorganizer_ajax_handler' function. This makes it possible for unauthenticated attackers to extract sensitive data including backups or other sensitive information if the files have been moved to the built-in Trash folder.	2024-06-07	7.5	CVE-2024-5599
solarwinds -- solarwinds_platform	The SolarWinds Platform was determined to be affected by a SWQL Injection Vulnerability. Attack complexity is high for this vulnerability.	2024-06-04	8.1	CVE-2024-28996
solarwinds -- solarwinds_platform	The SolarWinds Platform was determined to be affected by a Race Condition Vulnerability affecting the web console.	2024-06-04	8.1	CVE-2024-28999
SolarWinds -- SolarWinds Serv-U	SolarWinds Serv-U was susceptible to a directory transversal vulnerability that would allow access to read sensitive files on the host machine.	2024-06-06	8.6	CVE-2024-28995
sonalsinha21--SKT Addons for Elementor	The SKT Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Age Gate and Creative Slider widgets in all versions up to, and including, 2.0 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.	2024-06-08	7.4	CVE-2024-5091

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Summar Software--Mentor Employee Portal	Untrusted data deserialization vulnerability has been found in Mentor - Employee Portal, affecting version 3.83.35. This vulnerability could allow an attacker to execute arbitrary code, by injecting a malicious payload into the "ViewState" field.	2024-06-06	10	CVE-2024-5675 cve-
Sysaid--SysAid	SysAid - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	2024-06-06	9.9	CVE-2024-36393
Sysaid--SysAid	SysAid - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	2024-06-06	9.1	CVE-2024-36394
Tainacan.org--Tainacan	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Tainacan.Org Tainacan allows Reflected XSS.This issue affects Tainacan: from n/a through 0.21.3.	2024-06-03	7.1	CVE-2024-34794
Team Heateor--Heateor Social Login	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Team Heateor Heateor Social Login allows Cross-Site Scripting (XSS).This issue affects Heateor Social Login: from n/a through 1.1.32.	2024-06-08	7.1	CVE-2024-35706
Themeisle--Visualizer	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themeisle Visualizer.This issue affects Visualizer: from n/a through 3.11.1.	2024-06-08	8.5	CVE-2024-35736
themeum--Tutor LMS eLearning and online course solution	The Tutor LMS - eLearning and online course solution plugin for WordPress is vulnerable to time-based SQL Injection via the 'course_id' parameter in all versions up to, and including, 2.7.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with admin access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-06-07	7.2	CVE-2024-4902
ThimPress--Eduma	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ThimPress Eduma allows Reflected XSS.This issue affects Eduma: from n/a through 5.4.7.	2024-06-08	7.1	CVE-2024-35697
Tribulant--Newsletters	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Tribulant Newsletters allows Reflected XSS.This issue affects Newsletters: from n/a through 4.9.5.	2024-06-08	7.1	CVE-2024-35718
unitecms--Unlimited Elements For Elementor (Free Widgets, Addons, Templates)	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to blind SQL Injection via the 'data[addonID]' parameter in all versions up to, and including, 1.5.109 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.	2024-06-06	8.8	CVE-2024-5329
Unlimited Elements--Unlimited Elements For Elementor (Free Widgets, Addons, Templates)	Unrestricted Upload of File with Dangerous Type vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates) allows Code Injection.This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 1.5.66.	2024-06-04	9.1	CVE-2023-33930
userproplugin --userpro	Improper Privilege Management vulnerability in DeluxeThemes Userpro allows Privilege Escalation.This issue affects Userpro: from n/a through 5.1.8.	2024-06-04	9.8	CVE-2024-35700
vanyukov--Market Exporter	The Market Exporter plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'remove_files' function in all versions up to, and including, 2.0.19. This makes it possible for authenticated attackers, with Subscriber-level access and above, to use path traversal to delete arbitrary files on the server.	2024-06-07	7.5	CVE-2024-5637
viz-rs--nano-id	nano-id is a unique string ID generator for Rust. Affected versions of the nano-id crate incorrectly generated IDs using a reduced character set in the `nano_id::base62` and `nano_id::base58` functions. Specifically, the `base62` function used a character set of 32 symbols instead of the intended 62 symbols, and the `base58` function used a character set of 16 symbols instead of the intended 58 symbols. Additionally, the `nano_id::gen` macro is also affected when a custom character set that is not a power of 2 in size is specified. It should be noted that `nano_id::base64` is not affected by this vulnerability. This can result in a significant reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive	2024-06-04	9.4	CVE-2024-36400

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0.			
Wow-Company--Easy Digital Downloads Recent Purchases	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Wow-Company Easy Digital Downloads - Recent Purchases allows PHP Remote File Inclusion.This issue affects Easy Digital Downloads - Recent Purchases: from n/a through 1.0.2.	2024-06-04	9.6	CVE-2024-35629
wpase--Admin and Site Enhancements (ASE)	Improper Authentication vulnerability in wpase Admin and Site Enhancements (ASE) allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Admin and Site Enhancements (ASE): from n/a through 5.7.1.	2024-06-04	7.5	CVE-2023-46630
wpdevart--Responsive Image Gallery, Gallery Album	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in wpdevart Responsive Image Gallery, Gallery Album.This issue affects Responsive Image Gallery, Gallery Album: from n/a through 2.0.3.	2024-06-08	8.5	CVE-2024-35750
WPMobile.App--WPMobile.App	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPMobile.App allows Reflected XSS.This issue affects WPMobile.App: from n/a through 11.41.	2024-06-08	7.1	CVE-2024-35694
wshberlin--Startklar Elementor Addons	The Startklar Elementor Addons plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.7.15 via the 'dropzone_hash' parameter. This makes it possible for unauthenticated attackers to copy the contents of arbitrary files on the server, which can contain sensitive information, and to delete arbitrary directories, including the root WordPress directory.	2024-06-06	9.1	CVE-2024-5153
XforWooCommerce--XforWooCommerce	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in XforWooCommerce allows PHP Local File Inclusion.This issue affects XforWooCommerce: from n/a through 2.0.2.	2024-06-04	8.8	CVE-2024-33628
xootix--Login/Signup Popup (Inline Form + Woocommerce)	The Login/Signup Popup (Inline Form + Woocommerce) plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'import_settings' function in versions 2.7.1 to 2.7.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change arbitrary options on affected sites. This can be used to enable new user registration and set the default role for new users to Administrator.	2024-06-06	8.8	CVE-2024-5324
Yannick Lefebvre--Link Library	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Yannick Lefebvre Link Library link-library allows Reflected XSS.This issue affects Link Library: from n/a through 7.6.3.	2024-06-08	7.1	CVE-2024-35687
YdataAI--ydata-profiling	Deserialization of untrusted data can occur in versions 3.7.0 or newer of Ydata's ydata-profiling open-source library, enabling a malicously crafted report to run arbitrary code on an end user's system when loaded.	2024-06-04	7.8	CVE-2024-37062
YdataAI--ydata-profiling	A cross-site scripting (XSS) vulnerability in versions 3.7.0 or newer of Ydata's ydata-profiling open-source library allows for payloads to be run when a maliocusly crafted report is viewed in the browser.	2024-06-04	7.8	CVE-2024-37063
YdataAI--ydata-profiling	Deseriliazation of untrusted data can occur in versions 3.7.0 or newer of Ydata's ydata-profiling open-source library, enabling a maliciously crafted dataset to run arbitrary code on an end user's system when loaded.	2024-06-04	7.8	CVE-2024-37064
actpro --extra_product_options_for_woocommerce	Missing Authorization vulnerability in actpro Extra Product Options for WooCommerce.This issue affects Extra Product Options for WooCommerce: from n/a through 3.0.6.	2024-06-10	8.8	CVE-2024-35727
adfinis--document-merge-service	Document Merge Service is a document template merge service providing an API to manage templates and merge them with given data. Versions 6.5.1 and prior are vulnerable to remote code execution via server-side template injection which, when executed as root, can result in full takeover of the affected system. As of time of publication, no patched version exists, nor have any known workarounds been disclosed.	2024-06-11	9.9	CVE-2024-37301
Adobe--Adobe Commerce	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could result in arbitrary code execution. An attacker could exploit this vulnerability by sending a crafted XML document that references external entities. Exploitation of this issue does not require user interaction.	2024-06-13	9.8	CVE-2024-34102

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Adobe--Adobe Commerce	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction, but admin privileges are required	2024-06-13	9.1	CVE-2024-34108
Adobe--Adobe Commerce	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction, but attack complexity is high.	2024-06-13	8.1	CVE-2024-34103
Adobe--Adobe Commerce	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized access, leading to both confidentiality and integrity impact. Exploitation of this issue does not require user interaction.	2024-06-13	8.2	CVE-2024-34104
Adobe--Adobe Commerce	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction, but admin privileges are required.	2024-06-13	7.2	CVE-2024-34109
Adobe--Adobe Commerce	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution. A high-privilege attacker could exploit this vulnerability by uploading a malicious file to the system, which could then be executed. Exploitation of this issue does not require user interaction.	2024-06-13	7.2	CVE-2024-34110
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized access. Exploitation of this issue does not require user interaction.	2024-06-13	7.5	CVE-2024-26029
Adobe--Adobe Framemaker Publishing Server	Adobe Framemaker Publishing Server versions 2020.3, 2022.2 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction.	2024-06-13	10	CVE-2024-30299
Adobe--Adobe Framemaker Publishing Server	Adobe Framemaker Publishing Server versions 2020.3, 2022.2 and earlier are affected by an Information Exposure vulnerability (CWE-200) that could lead to privilege escalation. An attacker could exploit this vulnerability to gain access to sensitive information which may include system or user privileges. Exploitation of this issue does not require user interaction.	2024-06-13	9.8	CVE-2024-30300
Adobe--ColdFusion	ColdFusion versions 2023u7, 2021u13 and earlier are affected by an Improper Access Control vulnerability that could result in arbitrary file system read. An attacker could exploit this vulnerability to gain unauthorized access to sensitive files or data. Exploitation of this issue does not require user interaction.	2024-06-13	7.5	CVE-2024-34112
Adobe--Photoshop Desktop	Photoshop Desktop versions 24.7.3, 25.7 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.	2024-06-13	7.8	CVE-2024-20753
Adobe--Substance3D - Stager	Substance3D - Stager versions 2.1.4 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.	2024-06-13	7.8	CVE-2024-34115
aimeos--aimeos-core	Aimeos is an Open Source e-commerce framework for online shops. Starting in version 2024.01.1 and prior to version 2024.04.5, a user with administrative privileges can upload files that look like images but contain PHP code which can then be executed in the context of the web server. Version 2024.04.5 fixes the issue.	2024-06-11	7.2	CVE-2024-37295
apple -- macos	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Ventura 13.6.5, macOS Monterey 12.7.4. An app may be able to break out of its sandbox.	2024-06-10	8.6	CVE-2024-23299
apple -- macos	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Monterey 12.5. Processing a maliciously crafted tiff file may lead to arbitrary code execution.	2024-06-10	7.8	CVE-2022-32897
apple -- macos	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Monterey 12.5. Processing an AppleScript may result in unexpected termination or disclosure of process memory.	2024-06-10	7.1	CVE-2022-48578

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- macos	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Ventura 13. An app may be able to break out of its sandbox.	2024-06-10	7.8	CVE-2022-48683
arraytics--WP Timetics- AI-powered Appointment Booking Calendar and Online Scheduling Plugin	The Timetics- AI-powered Appointment Booking with Visual Seat Plan and ultimate Calendar Scheduling plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the make_staff() function in all versions up to, and including, 1.0.21. This makes it possible for unauthenticated attackers to grant users staff permissions.	2024-06-14	7.3	CVE-2024-1094
Aruphash--Crafthemes Demo Import	Missing Authentication for Critical Function vulnerability in Aruphash Crafthemes Demo Import allows Functionality Misuse.This issue affects Crafthemes Demo Import: from n/a through 3.3.	2024-06-10	7.6	CVE-2024-34800
arwebdesign -- dashboard_to-do_list	Missing Authorization vulnerability in Andrew Rapps Dashboard To-Do List.This issue affects Dashboard To-Do List: from n/a through 1.2.0.	2024-06-10	8.8	CVE-2024-35723
ASUS--Download Master	The upload functionality of ASUS Download Master does not properly filter user input. Remote attackers with administrative privilege can exploit this vulnerability to upload any file to any location. They may even upload malicious web page files to the website directory, allowing arbitrary system commands to be executed upon browsing the webpage.	2024-06-14	7.2	CVE-2024-31161
ASUS--Download Master	The specific function parameter of ASUS Download Master does not properly filter user input. An unauthenticated remote attacker with administrative privileges can exploit this vulnerability to execute arbitrary system commands on the device.	2024-06-14	7.2	CVE-2024-31162
ASUS--Download Master	ASUS Download Master has a buffer overflow vulnerability. An unauthenticated remote attacker with administrative privileges can exploit this vulnerability to execute arbitrary system commands on the device.	2024-06-14	7.2	CVE-2024-31163
ASUS--DSL-N17U	Certain models of ASUS routers have an arbitrary firmware upload vulnerability. An unauthenticated remote attacker can exploit this vulnerability to execute arbitrary system commands on the device.	2024-06-14	9.8	CVE-2024-3912
ASUS--ZenWiFi XT8	Certain ASUS router models have authentication bypass vulnerability, allowing unauthenticated remote attackers to log in the device.	2024-06-14	9.8	CVE-2024-3080
ASUS--ZenWiFi XT8	Certain models of ASUS routers have buffer overflow vulnerabilities, allowing remote attackers with administrative privileges to execute arbitrary commands on the device.	2024-06-14	7.2	CVE-2024-3079
avast -- antivirus	A sym-linked file accessed via the repair function in Avast Antivirus <24.2 on Windows may allow user to elevate privilege to delete arbitrary files or run processes as NT AUTHORITY\SYSTEM.Â The vulnerability exists within the "Repair" (settings -> troubleshooting -> repair) feature, which attempts to delete a file in the current user's AppData directory as NT AUTHORITY\SYSTEM. AÂ low-privileged user can make a pseudo-symlink and a junction folder and point to a file on the system. This can provide a low-privileged user an Elevation of Privilege to win a race-condition which will re-create the system files and make Windows callback to a specially-crafted file which could be used to launch a privileged shell instance. This issue affects Avast Antivirus prior to 24.2.	2024-06-10	7	CVE-2024-5102 security@nortonlifelock.com
awplife -- image_gallery	Missing Authorization vulnerability in A WP Life Image Gallery - Lightbox Gallery, Responsive Photo Gallery, Masonry Gallery.This issue affects Image Gallery - Lightbox Gallery, Responsive Photo Gallery, Masonry Gallery: from n/a through 1.4.5.	2024-06-10	8.8	CVE-2024-35721
awplife -- slider_responsive_slideshow	Missing Authorization vulnerability in A WP Life Slider Responsive Slideshow - Image slider, Gallery slideshow.This issue affects Slider Responsive Slideshow - Image slider, Gallery slideshow: from n/a through 1.4.0.	2024-06-10	8.8	CVE-2024-35722
awslabs--aws-deployment-framework	The AWS Deployment Framework (ADF) is a framework to manage and deploy resources across multiple AWS accounts and regions within an AWS Organization. ADF allows for staged, parallel, multi-account, cross-region deployments of applications or resources via the structure defined in AWS Organizations while taking advantage of services such as AWS CodePipeline, AWS CodeBuild, and AWS CodeCommit to alleviate the heavy lifting and management compared to a traditional CI/CD setup. ADF contains a bootstrap process that is responsible to deploy ADF's bootstrap stacks to facilitate multi-account cross-region deployments. The ADF bootstrap process relies on elevated privileges to perform this task. Two versions of the bootstrap process exist; a code-change driven pipeline using AWS	2024-06-11	7.5	CVE-2024-37293

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CodeBuild and an event-driven state machine using AWS Lambda. If an actor has permissions to change the behavior of the CodeBuild project or the Lambda function, they would be able to escalate their privileges. Prior to version 4.0.0, the bootstrap CodeBuild role provides access to the `sts:AssumeRole` operation without further restrictions. Therefore, it is able to assume into any AWS Account in the AWS Organization with the elevated privileges provided by the cross-account access role. By default, this role is not restricted when it is created by AWS Organizations, providing Administrator level access to the AWS resources in the AWS Account. The patches for this issue are included in `aws-deployment-framework` version 4.0.0. As a temporary mitigation, add a permissions boundary to the roles created by ADF in the management account. The permissions boundary should deny all IAM and STS actions. This permissions boundary should be in place until you upgrade ADF or bootstrap a new account. While the permissions boundary is in place, the account management and bootstrapping of accounts are unable to create, update, or assume into roles. This mitigates the privilege escalation risk, but also disables ADF's ability to create, manage, and bootstrap accounts.			
BlackBerry--QNX Software Development Platform	An improper input validation vulnerability in the SGI Image Codec of QNX SDP version(s) 6.6, 7.0, and 7.1 could allow an attacker to potentially cause a denial-of-service condition or execute code in the context of the image processing process.	2024-06-11	9	CVE-2024-35213 secure@blackberry.com
bosathemes -- bosa_elementor_addons_and_templates_for_woocommerce	Missing Authorization vulnerability in Bosa Themes Bosa Elementor Addons and Templates for WooCommerce.This issue affects Bosa Elementor Addons and Templates for WooCommerce: from n/a through 1.0.12.	2024-06-10	8.8	CVE-2024-35724
buddypress_cover_project -- buddypress_cover	Unrestricted Upload of File with Dangerous Type vulnerability in Asghar Hatampoor BuddyPress Cover allows Code Injection.This issue affects BuddyPress Cover: from n/a through 2.1.4.2.	2024-06-10	9.8	CVE-2024-35746
cilium--cilium	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Starting in version 1.13.0 and prior to versions 1.13.7, 1.14.12, and 1.15.6, the output of `cilium-bugtool` can contain sensitive data when the tool is run (with the `--envoy-dump` flag set) against Cilium deployments with the Envoy proxy enabled. Users of the TLS inspection, Ingress with TLS termination, Gateway API with TLS termination, and Kafka network policies with API key filtering features are affected. The sensitive data includes the CA certificate, certificate chain, and private key used by Cilium HTTP Network Policies, and when using Ingress/Gateway API and the API keys used in Kafka-related network policy. `cilium-bugtool` is a debugging tool that is typically invoked manually and does not run during the normal operation of a Cilium cluster. This issue has been patched in Cilium v1.15.6, v1.14.12, and v1.13.17. There is no workaround to this issue.	2024-06-13	7.9	CVE-2024-37307
cloudfoundry -- cf-deployment	Improper handling of requests in Routing Release > v0.273.0 and <= v0.297.0 allows an unauthenticated attacker to degrade the service availability of the Cloud Foundry deployment if performed at scale.	2024-06-10	7.5	CVE-2024-22279
codename065--Download Manager	The Download Manager plugin for WordPress is vulnerable to unauthorized access of data due to an improper authorization check on the 'protectMediaLibrary' function in all versions up to, and including, 3.2.89. This makes it possible for unauthenticated attackers to download password-protected files.	2024-06-13	7.5	CVE-2024-2098
codeparrots -- easy_forms_for_mailchimp	Missing Authorization vulnerability in Code Parrots Easy Forms for Mailchimp.This issue affects Easy Forms for Mailchimp: from n/a through 6.9.0.	2024-06-10	7.3	CVE-2024-35742
codepeople -- wp_time_slots_booking_form	Missing Authorization vulnerability in CodePeople WP Time Slots Booking Form.This issue affects WP Time Slots Booking Form: from n/a through 1.2.11.	2024-06-10	9.8	CVE-2024-35735
codexpert--CoDesigner The Most Compact and User-Friendly Elementor WooCommerce	The CoDesigner WooCommerce Builder for Elementor - Customize Checkout, Shop, Email, Products & More plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 4.4.1 via deserialization of untrusted input from the recently_viewed_products cookie. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the	2024-06-13	9	CVE-2024-4371

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Builder	target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.			
composer--composer	Composer is a dependency manager for PHP. On the 2.x branch prior to versions 2.2.24 and 2.7.7, the `status`, `reinstall` and `remove` commands with packages installed from source via git containing specially crafted branch names in the repository can be used to execute code. Patches for this issue are available in version 2.2.24 for 2.2 LTS or 2.7.7 for mainline. As a workaround, avoid installing dependencies via git by using `--prefer-dist` or the `preferred-install: dist` config setting.	2024-06-10	8.8	CVE-2024-35241
composer--composer	Composer is a dependency manager for PHP. On the 2.x branch prior to versions 2.2.24 and 2.7.7, the `composer install` command running inside a git/hg repository which has specially crafted branch names can lead to command injection. This requires cloning untrusted repositories. Patches are available in version 2.2.24 for 2.2 LTS or 2.7.7 for mainline. As a workaround, avoid cloning potentially compromised repositories.	2024-06-10	8.8	CVE-2024-35242
Comtrend--Comtrend WLD71-T1_v2.0.201820	Command injection vulnerability in Comtrend router WLD71-T1_v2.0.201820, affecting the GRG-4280us version. This vulnerability could allow an authenticated user to execute commands inside the router by making a POST request to the URL "/boaform/admin/formUserTracert".	2024-06-10	8	CVE-2024-5785 cve-
Consensu.IO--Consensu.io	Missing Authorization vulnerability in Consensu.IO Consensu.Io.This issue affects Consensu.Io: from n/a through 1.0.1.	2024-06-12	7.5	CVE-2023-48280
contrid--Slideshow Gallery LITE	The Slideshow Gallery LITE plugin for WordPress is vulnerable to time-based SQL Injection via the id parameter in all versions up to, and including, 1.8.1 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 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.	2024-06-12	8.1	CVE-2024-5543
cvat-ai--cvat	Computer Vision Annotation Tool (CVAT) is an interactive video and image annotation tool for computer vision. CVAT allows users to supply custom endpoint URLs for cloud storages based on Amazon S3 and Azure Blob Storage. Starting in version 2.1.0 and prior to version 2.14.3, an attacker with a CVAT account can exploit this feature by specifying URLs whose host part is an intranet IP address or an internal domain name. By doing this, the attacker may be able to probe the network that the CVAT backend runs in for HTTP(S) servers. In addition, if there is a web server on this network that is sufficiently API-compatible with an Amazon S3 or Azure Blob Storage endpoint, and either allows anonymous access, or allows authentication with credentials that are known by the attacker, then the attacker may be able to create a cloud storage linked to this server. They may then be able to list files on the server; extract files from the server, if these files are of a type that CVAT supports reading from cloud storage (media data (such as images/videos/archives), importable annotations or datasets, task/project backups); and/or overwrite files on this server with exported annotations/datasets/backups. The exact capabilities of the attacker will depend on how the internal server is configured. Users should upgrade to CVAT 2.14.3 to receive a patch. In this release, the existing SSRF mitigation measures are applied to requests to cloud providers, with access to intranet IP addresses prohibited by default. Some workarounds are also available. One may use network security solutions such as virtual networks or firewalls to prohibit network access from the CVAT backend to unrelated servers on your internal network and/or require authentication for access to internal servers.	2024-06-13	7.1	CVE-2024-37164
cvat-ai--cvat	Computer Vision Annotation Tool (CVAT) is an interactive video and image annotation tool for computer vision. Starting in version 2.2.0 and prior to version 2.14.3, if an attacker can trick a logged-in CVAT user into visiting a malicious URL, they can initiate a dataset export or a backup from a project, task or job that the victim user has permission to export into a cloud storage that the victim user has access to. The name of the resulting file can be chosen by the attacker. This implies that the attacker can overwrite arbitrary files in any cloud storage that the victim can access and, if the attacker has read access to the cloud storage used in the attack, they can obtain media files, annotations, settings and other information from any projects, tasks or jobs that the victim has permission to export. Version 2.14.3 contains a fix for the issue. No known workarounds are available.	2024-06-13	7.1	CVE-2024-37306

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Dell--Common Event Enabler	Dell Common Event Enabler, version 8.9.10.0 and prior, contain an insecure deserialization vulnerability in CAVATools. A local unauthenticated attacker could potentially exploit this vulnerability, leading to arbitrary code execution in the context of the logged in user. Exploitation of this issue requires a victim to open a malicious file.	2024-06-12	7.8	CVE-2024-28964
Dell--CPG BIOS	Dell Client Platform BIOS contains an Improper Input Validation vulnerability in an externally developed component. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution.	2024-06-13	7.5	CVE-2024-32858
Dell--CPG BIOS	Dell Client Platform BIOS contains an Improper Input Validation vulnerability in an externally developed component. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution.	2024-06-13	7.5	CVE-2024-32859
Dell--CPG BIOS	Dell Client Platform BIOS contains an Improper Input Validation vulnerability in an externally developed component. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution.	2024-06-13	7.5	CVE-2024-32860
Dell--Dell OpenManage Server Administrator	Dell OpenManage Server Administrator, versions 11.0.1.0 and prior, contains a Local Privilege Escalation vulnerability via XSL Hijacking. A local low-privileged malicious user could potentially exploit this vulnerability and escalate their privilege to the admin user and gain full control of the machine. Exploitation may lead to a complete system compromise.	2024-06-11	7.3	CVE-2024-37130
Dell--Secure Connect Gateway (SCG) Policy Manager	SCG Policy Manager, all versions, contains an overly permissive Cross-Origin Resource Policy (CORP) vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to the execution of malicious actions on the application in the context of the authenticated user.	2024-06-13	7.5	CVE-2024-37131
Dell--SmartFabric OS10 Software	Dell OS10 Networking Switches, versions10.5.6.x, 10.5.5.x, 10.5.4.x and 10.5.3.x ,contain an improper authorization vulnerability. A remote authenticated attacker could potentially exploit this vulnerability leading to escalation of privileges.	2024-06-12	8.8	CVE-2024-25949
Dell--Wyse 5070 Thin Client	Telemetry Dashboard v1.0.0.8 for Dell ThinOS 2402 contains a sensitive information disclosure vulnerability. An unauthenticated user with local access to the device could exploit this vulnerability leading to information disclosure.	2024-06-13	7.5	CVE-2024-30472
dreryk -- gabinet	Use of hard-coded password to the patients' database allows an attacker to retrieve sensitive data stored in the database. The password is the same among allÂ drEryk Gabinet installations.This issue affects drEryk Gabinet software versions from 7.0.0.0 through 9.17.0.0.	2024-06-10	9.8	CVE-2024-3699
estomed -- simple_care	Use of hard-coded password to the patients' database allows an attacker to retrieve sensitive data stored in the database. The password is the same among all Simple Care software installations. This issue affectsÂ Estomed Sp. z o.o. Simple Care software in all versions. The software is no longer supported.	2024-06-10	9.8	CVE-2024-3700
eurosoft -- przychodnia	Use of hard-coded password to the patients' database allows an attacker to retrieve sensitive data stored in the database. The password is the same among all Eurosoft Przychodnia installations. This issue affects Eurosoft Przychodnia software beforeÂ versionÂ 20240417.001 (from that version vulnerability is fixed).	2024-06-10	9.8	CVE-2024-1228
flightbycanto--Canto	The Canto plugin for WordPress is vulnerable to Remote File Inclusion in all versions up to, and including, 3.0.8 via the abspath parameter. This makes it possible for unauthenticated attackers to include remote files on the server, resulting in code execution. This required allow_url_include to be enabled on the target site in order to exploit.	2024-06-14	9.8	CVE-2024-4936
FooEvents--FooEvents for WooCommerce	The FooEvents for WooCommerce plugin for WordPress is vulnerable to unauthorized arbitrary file uploads due to an improper capability setting on the 'display_ticket_themes_page' function in versions up to, and including, 1.19.20. This makes it possible for authenticated attackers with contributor-level capabilities or above, to upload arbitrary files on the affected site's server which may make remote code execution possible. This was partially patched in 1.19.20, and fully patched in 1.19.21.	2024-06-15	7.1	CVE-2024-6000
Fortinet--FortiOS	A stack-based buffer overflow in Fortinet FortiOS version 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 all versions allows attacker to execute unauthorized code or commands via specially crafted commands	2024-06-11	7.8	CVE-2024-23110
Fortinet--FortiPAM	A stack-based buffer overflow in Fortinet FortiPAM version 1.2.0, 1.1.0 through 1.1.2, 1.0.0 through 1.0.3, FortiWeb, FortiAuthenticator, FortiSwitchManager version 7.2.0 through 7.2.3, 7.0.1 through 7.0.3, FortiOS version 7.4.0 through 7.4.3, 7.2.0 through 7.2.7, 7.0.0 through 7.0.14, 6.4.0 through 6.4.15, 6.2.0 through 6.2.16, 6.0.0 through 6.0.18, FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.9, 7.0.0 through 7.0.15, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0	2024-06-11	7.5	CVE-2024-26010

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	through 1.1.6, 1.0.0 through 1.0.7 allows attacker to execute unauthorized code or commands via specially crafted packets.			
Fuji Electric--Tellus Lite V-Simulator	Fuji Electric Tellus Lite V-Simulator is vulnerable to an out-of-bounds write, which could allow an attacker to manipulate memory, resulting in execution of arbitrary code.	2024-06-13	7.8	CVE-2024-37022
Fuji Electric--Tellus Lite V-Simulator	Fuji Electric Tellus Lite V-Simulator is vulnerable to a stack-based buffer overflow, which could allow an attacker to execute arbitrary code.	2024-06-13	7.8	CVE-2024-37029
fujielectric -- monitouch_v-sft	Fuji Electric Monitouch V-SFTÂ is vulnerable to a type confusion, which could cause a crash or code execution.	2024-06-10	9.8	CVE-2024-5597
getawesomesupport -- awesome_support	Missing Authorization vulnerability in Awesome Support Team Awesome Support.This issue affects Awesome Support: from n/a through 6.1.7.	2024-06-10	8.8	CVE-2024-35741
google -- android	there is a possible way to bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2024-06-13	7.8	CVE-2024-32896 dsap-vuln-management@google.com
Guangdong Baolun Electronics--IP Network Broadcasting Service Platform	A vulnerability was found in Guangdong Baolun Electronics IP Network Broadcasting Service Platform 2.0. It has been classified as critical. Affected is an unknown function of the file /api/v2/maps. The manipulation of the argument orderColumn 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-268692. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-14	7.3	CVE-2024-6003
gurgunday--ghtml	ghtml is software that uses tagged templates for template engine functionality. It is possible to introduce user-controlled JavaScript code and trigger a Cross-Site Scripting (XSS) vulnerability in some cases. Version 2.0.0 introduces changes to mitigate this issue. Version 2.0.0 contains updated documentation to clarify that while ghtml escapes characters with special meaning in HTML, it does not provide comprehensive protection against all types of XSS attacks in every scenario. This aligns with the approach taken by other template engines. Developers should be cautious and take additional measures to sanitize user input and prevent potential vulnerabilities. Additionally, the backtick character (`) is now also escaped to prevent the creation of strings in most cases where a malicious actor somehow gains the ability to write JavaScript. This does not provide comprehensive protection either.	2024-06-10	8.9	CVE-2024-37166
hakeemnala--Build App Online	The Build App Online plugin for WordPress is vulnerable to account takeover due to a weak password reset mechanism in all versions up to, and including, 1.0.21. This makes it possible for unauthenticated attackers to reset the password of arbitrary users by guessing an 4-digit numeric reset code.	2024-06-11	8.1	CVE-2023-7264
Hitachi Energy--FOXMAN-UN	An authentication bypass vulnerability exists in the FOXMAN-UN/UNEM server / API Gateway component that if exploited allows attackers without any access to interact with the services and the post-authentication attack surface.	2024-06-11	10	CVE-2024-2013
Hitachi Energy--FOXMAN-UN	vulnerability exists in the FOXMAN-UN/UNEM server / API Gateway that if exploited an attacker could use to allow unintended commands or code to be executed on the UNEM server allowing sensitive data to be read or modified or could cause other unintended behavior	2024-06-11	9.1	CVE-2024-2012
Hitachi Energy--FOXMAN-UN	A heap-based buffer overflow vulnerability exists in the FOXMAN-UN/UNEM that if exploited will generally lead to a denial of service but can be used to execute arbitrary code, which is usually outside the scope of a program's implicit security policy	2024-06-11	8.6	CVE-2024-2011
Hitachi Energy--FOXMAN-UN	A user/password reuse vulnerability exists in the FOXMAN-UN/UNEMÂ application and server management. If exploited a malicious user could use the passwords and login information to extend access on the server and other services.	2024-06-11	8	CVE-2024-28020
Hitachi Energy--FOXMAN-UN	A vulnerability exists in the FOXMAN-UN/UNEM server that affects the message queueing mechanism's certificate validation. If exploited an attacker could spoof a trusted entity causing a loss of confidentiality and integrity.	2024-06-11	8	CVE-2024-28021
Huawei--HarmonyOS	Privilege escalation vulnerability in the AMS module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2024-06-14	7.8	CVE-2024-36500
Huawei--HarmonyOS	Out-of-bounds read vulnerability in the audio module Impact: Successful exploitation of this vulnerability will affect availability.	2024-06-14	7.9	CVE-2024-36502

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Huawei--HarmonyOS	Memory management vulnerability in the Gralloc module Impact: Successful exploitation of this vulnerability will affect availability.	2024-06-14	7.3	CVE-2024-36503
IBM--i	IBM i 7.2, 7.3, 7.4, and 7.5 contains a local privilege escalation vulnerability caused by an insufficient authority requirement. A local user without administrator privilege can configure a physical file trigger to execute with the privileges of a user socially engineered to access the target file. The correction is to require administrator privilege to configure trigger support. IBM X-Force ID: 285203.	2024-06-15	7.4	CVE-2024-27275
icegram--Email Subscribers by Icegram Express Email Marketing, Newsletters, Automation for WordPress & WooCommerce	The Icegram Express plugin for WordPress is vulnerable to SQL Injection via the 'options[list_id]' parameter in all versions up to, and including, 5.7.22 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.	2024-06-12	8.8	CVE-2024-4845
instawp--InstaWP Connect 1-click WP Staging & Migration	The InstaWP Connect - 1-click WP Staging & Migration plugin for WordPress is vulnerable to arbitrary option updates due to a missing authorization checks on the REST API calls in all versions up to, and including, 0.1.0.38. This makes it possible for unauthenticated attackers to connect the site to InstaWP API, edit arbitrary site options and create administrator accounts.	2024-06-12	9.8	CVE-2024-4898
ipages_flipbook_project -- ipages_flipbook	Missing Authorization vulnerability in Avirtum iPages Flipbook.This issue affects iPages Flipbook: from n/a through 1.5.1.	2024-06-10	7.3	CVE-2024-4744
itsourcecode--Online Bookstore	A vulnerability was found in itsourcecode Online Bookstore 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file bookPerPub.php. The manipulation of the argument pubid 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-268459.	2024-06-14	7.3	CVE-2024-5983
itsourcecode--Online Bookstore	A vulnerability was found in itsourcecode Online Bookstore 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file book.php. The manipulation of the argument bookisbn 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-268460.	2024-06-14	7.3	CVE-2024-5984
jetbrains -- aqua	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4	2024-06-10	7.5	CVE-2024-37051
jupyterhub--jupyter-server-proxy	Jupyter Server Proxy allows users to run arbitrary external processes alongside their notebook server and provide authenticated web access to them. Versions of 3.x prior to 3.2.4 and 4.x prior to 4.2.0 have a reflected cross-site scripting (XSS) issue. The `/proxy` endpoint accepts a `host` path segment in the format `/proxy/<host>`. When this endpoint is called with an invalid `host` value, `jupyter-server-proxy` replies with a response that includes the value of `host`, without sanitization [2]. A third-party actor can leverage this by sending a phishing link with an invalid `host` value containing custom JavaScript to a user. When the user clicks this phishing link, the browser renders the response of `GET /proxy/<host>`, which runs the custom JavaScript contained in `host` set by the actor. As any arbitrary JavaScript can be run after the user clicks on a phishing link, this issue permits extensive access to the user's JupyterLab instance for an actor. Patches are included in versions 4.2.0 and 3.2.4. As a workaround, server operators who are unable to upgrade can disable the `jupyter-server-proxy` extension.	2024-06-11	9.6	CVE-2024-35225
jupyterhub--oauthenticator	OAuthenticator is software that allows OAuth2 identity providers to be plugged in and used with JupyterHub. JupyterHub < 5.0, when used with `GlobusOAuthenticator`, could be configured to allow all users from a particular institution only. This worked fine prior to JupyterHub 5.0, because `allow_all` did	2024-06-12	8.1	CVE-2024-37300

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	not take precedence over `identity_provider`. Since JupyterHub 5.0, `allow_all` does take precedence over `identity_provider`. On a hub with the same config, now all users will be allowed to login, regardless of `identity_provider`. `identity_provider` will basically be ignored. This is a documented change in JupyterHub 5.0, but is likely to catch many users by surprise. OAuthenticator 16.3.1 fixes the issue with JupyterHub 5.0, and does not affect previous versions. As a workaround, do not upgrade to JupyterHub 5.0 when using `GlobusOAuthenticator` in the prior configuration.			
la-studioweb -- element_kit_for_elementor	Missing Authorization vulnerability in LA-Studio LA-Studio Element Kit for Elementor.This issue affects LA-Studio Element Kit for Elementor: from n/a through 1.3.6.	2024-06-10	8.8	CVE-2024-35725
langflow -- langflow	Langflow through 0.6.19 allows remote code execution if untrusted users are able to reach the "POST /api/v1/custom_component" endpoint and provide a Python script.	2024-06-10	9.8	CVE-2024-37014
latepoint--LatePoint Plugin	The LatePoint Plugin plugin for WordPress is vulnerable to unauthorized access of data and modification of data due to a missing capability check on the 'start_or_use_session_for_customer' function in all versions up to and including 4.9.9. This makes it possible for unauthenticated attackers to view other customer's cabinets, including the ability to view PII such as email addresses and to change their LatePoint user password, which may or may not be associated with a WordPress account.	2024-06-14	9.1	CVE-2024-2472
Lenovo--Service Bridge	A privilege escalation vulnerability was reported in Lenovo Service Bridge prior to version 5.0.2.17 that could allow operating system commands to be executed if a specially crafted link is visited.	2024-06-13	7.5	CVE-2024-4696
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: net: fix __dst_negative_advice() race __dst_negative_advice() does not enforce proper RCU rules when sk->dst_cache must be cleared, leading to possible UAF. RCU rules are that we must first clear sk->sk_dst_cache, then call dst_release(old_dst). Note that sk_dst_reset(sk) is implementing this protocol correctly, while __dst_negative_advice() uses the wrong order. Given that ip6_negative_advice() has special logic against RTF_CACHE, this means each of the three ->negative_advice() existing methods must perform the sk_dst_reset() themselves. Note the check against NULL dst is centralized in __dst_negative_advice(), there is no need to duplicate it in various callbacks. Many thanks to Clement Lecigne for tracking this issue. This old bug became visible after the blamed commit, using UDP sockets.	2024-06-10	7.8	CVE-2024-36971
lnbits--lnbits	LNbits is a Lightning wallet and accounts system. Paying invoices in Eclair that do not get settled within the internal timeout (about 30s) lead to a payment being considered failed, even though it may still be in flight. This vulnerability can lead to a total loss of funds for the node backend. This vulnerability is fixed in 0.12.6.	2024-06-14	8.1	CVE-2024-34694
mcnardelli--Where I Was, Where I Will Be	The Where I Was, Where I Will Be plugin for WordPress is vulnerable to Remote File Inclusion in version <= 1.1.1 via the WIW_HEADER parameter of the /system/include/include_user.php file. This makes it possible for unauthenticated attackers to include and execute arbitrary files hosted on external servers, 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. This requires allow_url_include to be set to true in order to exploit, which is not commonly enabled.	2024-06-14	9.8	CVE-2024-5577
melapress -- melapress_login_security	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Melapress MelaPress Login Security allows PHP Remote File Inclusion.This issue affects MelaPress Login Security: from n/a through 1.3.0.	2024-06-10	7.2	CVE-2024-35650
MicroDicom--DICOM Viewer	MicroDicom DICOM Viewer is vulnerable to a stack-based buffer overflow, which may allow an attacker to execute arbitrary code on affected installations of DICOM Viewer. User interaction is required to exploit this vulnerability.	2024-06-11	8.8	CVE-2024-28877
MicroDicom--DICOM Viewer	An attacker could retrieve sensitive files (medical images) as well as plant new medical images or overwrite existing medical images on a MicroDicom DICOM Viewer system. User interaction is required to exploit this vulnerability.	2024-06-11	8.8	CVE-2024-33606
microsoft -- windows_10_1507	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	2024-06-11	9.8	CVE-2024-30080
Microsoft--Azure Data Science	Azure Science Virtual Machine (DSVM) Elevation of Privilege Vulnerability	2024-06-11	8.1	CVE-2024-37325

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Virtual Machines				
Microsoft--Azure Monitor	Azure Monitor Agent Elevation of Privilege Vulnerability	2024-06-11	7.1	CVE-2024-35254
Microsoft--Azure Storage	Azure Storage Movement Client Library Denial of Service Vulnerability	2024-06-11	7.5	CVE-2024-35252
Microsoft--Microsoft 365 Apps for Enterprise	Microsoft Office Remote Code Execution Vulnerability	2024-06-11	7.5	CVE-2024-30101
Microsoft--Microsoft 365 Apps for Enterprise	Microsoft Office Remote Code Execution Vulnerability	2024-06-11	7.3	CVE-2024-30102
Microsoft--Microsoft Dynamics 365 Business Central 2023 Release Wave 1	Microsoft Dynamics 365 Business Central Elevation of Privilege Vulnerability	2024-06-11	7.3	CVE-2024-35248
Microsoft--Microsoft Dynamics 365 Business Central 2024 Release Wave 1	Microsoft Dynamics 365 Business Central Remote Code Execution Vulnerability	2024-06-11	8.8	CVE-2024-35249
Microsoft--Microsoft Office 2019	Microsoft Outlook Remote Code Execution Vulnerability	2024-06-11	8.8	CVE-2024-30103
Microsoft--Microsoft Office 2019	Microsoft Office Remote Code Execution Vulnerability	2024-06-11	7.8	CVE-2024-30104
Microsoft--Microsoft SharePoint Enterprise Server 2016	Microsoft SharePoint Server Remote Code Execution Vulnerability	2024-06-11	7.8	CVE-2024-30100
Microsoft--Windows 10 Version 1809	Windows Kernel Elevation of Privilege Vulnerability	2024-06-11	8.8	CVE-2024-30068
Microsoft--Windows 10 Version 1809	Windows OLE Remote Code Execution Vulnerability	2024-06-11	8	CVE-2024-30077
Microsoft--Windows 10 Version 1809	Windows Wi-Fi Driver Remote Code Execution Vulnerability	2024-06-11	8.8	CVE-2024-30078
Microsoft--Windows 10 Version 1809	Microsoft Speech Application Programming Interface (SAPI) Remote Code Execution Vulnerability	2024-06-11	8.8	CVE-2024-30097
Microsoft--Windows 10 Version 1809	Win32k Elevation of Privilege Vulnerability	2024-06-11	7.8	CVE-2024-30082

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows 10 Version 1809	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	2024-06-11	7	CVE-2024-30084
Microsoft--Windows 10 Version 1809	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	2024-06-11	7.8	CVE-2024-30086
Microsoft--Windows 10 Version 1809	Win32k Elevation of Privilege Vulnerability	2024-06-11	7.8	CVE-2024-30087
Microsoft--Windows 10 Version 1809	Windows Kernel Elevation of Privilege Vulnerability	2024-06-11	7	CVE-2024-30088
Microsoft--Windows 10 Version 1809	Microsoft Streaming Service Elevation of Privilege Vulnerability	2024-06-11	7.8	CVE-2024-30089
Microsoft--Windows 10 Version 1809	Microsoft Streaming Service Elevation of Privilege Vulnerability	2024-06-11	7	CVE-2024-30090
Microsoft--Windows 10 Version 1809	Win32k Elevation of Privilege Vulnerability	2024-06-11	7.8	CVE-2024-30091
Microsoft--Windows 10 Version 1809	Windows Storage Elevation of Privilege Vulnerability	2024-06-11	7.3	CVE-2024-30093
Microsoft--Windows 10 Version 1809	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-06-11	7.8	CVE-2024-30094
Microsoft--Windows 10 Version 1809	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-06-11	7.8	CVE-2024-30095
Microsoft--Windows 10 Version 1809	Windows Kernel Elevation of Privilege Vulnerability	2024-06-11	7	CVE-2024-30099
Microsoft--Windows 10 Version 1809	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	2024-06-11	7.8	CVE-2024-35250
Microsoft--Windows 10 Version 1809	Windows Perception Service Elevation of Privilege Vulnerability	2024-06-11	7	CVE-2024-35265
Microsoft--Windows 11 version 21H2	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	2024-06-11	7.8	CVE-2024-30085
Microsoft--Windows 11 version 22H2	Microsoft Event Trace Log File Parsing Remote Code Execution Vulnerability	2024-06-11	7.8	CVE-2024-30072
Microsoft--Windows Server 2008 Service Pack 2	Windows Link Layer Topology Discovery Protocol Remote Code Execution Vulnerability	2024-06-11	8	CVE-2024-30074

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows Server 2008 Service Pack 2	Windows Link Layer Topology Discovery Protocol Remote Code Execution Vulnerability	2024-06-11	8	CVE-2024-30075
Microsoft--Windows Server 2019	Windows Standards-Based Storage Management Service Remote Code Execution Vulnerability	2024-06-11	7.8	CVE-2024-30062
Microsoft--Windows Server 2019	DHCP Server Service Denial of Service Vulnerability	2024-06-11	7.5	CVE-2024-30070
Microsoft--Windows Server 2019	Windows Standards-Based Storage Management Service Denial of Service Vulnerability	2024-06-11	7.5	CVE-2024-30083
Microsoft--Windows Server 2022	Windows Kernel Elevation of Privilege Vulnerability	2024-06-11	8.8	CVE-2024-30064
MultiVendorX--WC Marketplace	Missing Authorization vulnerability in MultiVendorX WC Marketplace.This issue affects WC Marketplace: from n/a through 4.0.25.	2024-06-11	8.6	CVE-2024-24703
n/a--n/a	An issue was discovered in Samsung Mobile Processor Exynos 2200, Exynos 1480, Exynos 2400. It lacks proper buffer length checking, which can result in an Out-of-Bounds Write.	2024-06-13	8.4	CVE-2024-31956
n/a--n/a	An issue was discovered in Samsung Mobile Processor and Wearable Processor Exynos 850, Exynos 1080, Exynos 2100, Exynos 1280, Exynos 1380, Exynos 1330, Exynos W920, Exynos W930. The mobile processor lacks proper length checking, which can result in an OOB (Out-of-Bounds) Write vulnerability.	2024-06-13	8.4	CVE-2024-32504
nextcloud--security-advisories	Nextcloud Server is a self hosted personal cloud system. A recipient of a share with read&share permissions could reshare the item with more permissions. It is recommended that the Nextcloud Server is upgraded to 26.0.13 or 27.1.8 or 28.0.4 and that the Nextcloud Enterprise Server is upgraded to 26.0.13 or 27.1.8 or 28.0.4.	2024-06-14	8.1	CVE-2024-37882
nextcloud--security-advisories	Nextcloud server is a self hosted personal cloud system. Under some circumstance it was possible to bypass the second factor of 2FA after successfully providing the user credentials. It is recommended that the Nextcloud Server is upgraded to 26.0.13, 27.1.8 or 28.0.4 and Nextcloud Enterprise Server is upgraded to 21.0.9.17, 22.2.10.22, 23.0.12.17, 24.0.12.13, 25.0.13.8, 26.0.13, 27.1.8 or 28.0.4.	2024-06-14	7.3	CVE-2024-37313
nvidia--GPU display driver, vGPU software, and Cloud Gaming	NVIDIA GPU Display Driver for Windows contains a vulnerability where the information from a previous client or another process could be disclosed. A successful exploit of this vulnerability might lead to code execution, information disclosure, or data tampering.	2024-06-13	7.8	CVE-2024-0089
nvidia--GPU display driver, vGPU software, and Cloud Gaming	NVIDIA GPU driver for Windows and Linux contains a vulnerability where a user can cause an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	2024-06-13	7.8	CVE-2024-0090
nvidia--GPU display driver, vGPU software, and Cloud Gaming	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability where a user can cause an untrusted pointer dereference by executing a driver API. A successful exploit of this vulnerability might lead to denial of service, information disclosure, and data tampering.	2024-06-13	7.8	CVE-2024-0091
nvidia--NVIDIA Triton Inference Server	NVIDIA Triton Inference Server for Linux and Windows contains a vulnerability where a user can inject forged logs and executable commands by injecting arbitrary data as a new log entry. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	2024-06-13	9	CVE-2024-0095
nvidia--vGPU software and Cloud Gaming	NVIDIA vGPU software for Linux contains a vulnerability in the Virtual GPU Manager, where the guest OS could execute privileged operations. A successful exploit of this vulnerability might lead to information disclosure, data tampering, escalation of privileges, and denial of service.	2024-06-13	7.8	CVE-2024-0084

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nvidia--vGPU software and Cloud Gaming	NVIDIA vGPU software for Linux contains a vulnerability in the Virtual GPU Manager, where the guest OS could cause buffer overrun in the host. A successful exploit of this vulnerability might lead to information disclosure, data tampering, escalation of privileges, and denial of service.	2024-06-13	7.8	CVE-2024-0099
OpenText--ArcSight Logger	Stored Cross-Site Scripting (XSS) vulnerabilities have been identified in OpenText ArcSight Logger. The vulnerabilities could be remotely exploited.	2024-06-11	8.1	CVE-2024-4190
oretnom23 -- online_medicine_ordering_system	Sourcecodester Online Medicine Ordering System 1.0 is vulnerable to Arbitrary file deletion vulnerability as the backend settings have the function of deleting pictures to delete any files.	2024-06-10	9.1	CVE-2024-32167
parisneo -- lollms_web_ui	A Cross-Site Request Forgery (CSRF) vulnerability exists in the clear_personality_files_list function of the parisneo/lollms-webui v9.6. The vulnerability arises from the use of a GET request to clear personality files list, which lacks proper CSRF protection. This flaw allows attackers to trick users into performing actions without their consent, such as deleting important files on the system. The issue is present in the application's handling of requests, making it susceptible to CSRF attacks that could lead to unauthorized actions being performed on behalf of the user.	2024-06-10	8.1	CVE-2024-4328
popupbuilder--Popup Builder Create highly converting, mobile friendly marketing popups.	The Popup Builder - Create highly converting, mobile friendly marketing popups. 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, 4.3.1. While some functions contain a nonce check, the nonce can be obtained from the profile page of a logged-in user. This allows subscribers to perform several actions including deleting subscribers and perform blind Server-Side Request Forgery.	2024-06-15	8.1	CVE-2023-6696
popupbuilder--Popup Builder Create highly converting, mobile friendly marketing popups.	The Popup Builder plugin for WordPress is vulnerable to unauthorized modification of data and loss of data due to a missing capability check on all AJAX actions. This makes it possible for authenticated attackers, with subscriber-level access and above, to perform multiple unauthorized actions, such as deleting subscribers, and importing subscribers to conduct stored cross-site scripting attacks.	2024-06-15	7.4	CVE-2024-2544
Post SMTP--Post SMTP Mailer/Email Log	Missing Authorization vulnerability in Post SMTP Post SMTP Mailer/Email Log.This issue affects Post SMTP Mailer/Email Log: from n/a through 2.8.6.	2024-06-11	8.6	CVE-2023-52233
pq-crystals -- kyber	The Kyber reference implementation before 9b8d306, when compiled by LLVM Clang through 18.x with some common optimization options, has a timing side channel that allows attackers to recover an ML-KEM 512 secret key in minutes. This occurs because poly_frommsg in poly.c does not prevent Clang from emitting a vulnerable secret-dependent branch.	2024-06-10	7.5	CVE-2024-37880
pr-gateway--Blog2Social: Social Media Auto Post & Scheduler	The Blog2Social: Social Media Auto Post & Scheduler plugin for WordPress is vulnerable to SQL Injection via the 'b2sSortPostType' parameter in all versions up to, and including, 7.4.1 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 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.	2024-06-11	9.9	CVE-2024-3549
Premio--Folders Pro	The Folders Pro plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'handle_folders_file_upload' function in all versions up to, and including, 3.0.2. This makes it possible for authenticated attackers, with author access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-06-14	8.8	CVE-2024-2024
Red Hat--Red Hat Certificate System 10	A flaw was found in dogtag-pki and pki-core. The token authentication scheme can be bypassed with a LDAP injection. By passing the query string parameter sessionID=*, an attacker can authenticate with an existing session saved in the LDAP directory server, which may lead to escalation of privilege.	2024-06-11	7.5	CVE-2023-4727
Red Hat--Red Hat Enterprise Linux 7	A vulnerability was found in FreeIPA in a way when a Kerberos TGS-REQ is encrypted using the client's session key. This key is different for each new session, which protects it from brute force attacks. However, the ticket it contains is encrypted using the target principal key directly. For user principals, this key is a hash of a public per-principal randomly-generated salt and the user's password. If a principal is compromised it means the attacker would be able to retrieve tickets encrypted to any principal, all of them being encrypted by their own key directly.	2024-06-12	8.1	CVE-2024-3183

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	By taking these tickets and salts offline, the attacker could run brute force attacks to find character strings able to decrypt tickets when combined to a principal salt (i.e. find the principal's password).			
Red Hat--Red Hat Enterprise Linux 8	A vulnerability was found in FreeIPA in how the initial implementation of MS-SFU by MIT Kerberos was missing a condition for granting the "forwardable" flag on S4U2Self tickets. Fixing this mistake required adding a special case for the check_allowed_to_delegate() function: If the target service argument is NULL, then it means the KDC is probing for general constrained delegation rules and not checking a specific S4U2Proxy request. In FreeIPA 4.11.0, the behavior of ipadb_match_acl() was modified to match the changes from upstream MIT Kerberos 1.20. However, a mistake resulting in this mechanism applies in cases where the target service argument is set AND where it is unset. This results in S4U2Proxy requests being accepted regardless of whether or not there is a matching service delegation rule.	2024-06-12	7.1	CVE-2024-2698
Red Hat--Red Hat OpenShift Container Platform 4.15	A flaw was found in cri-o. A malicious container can create a symbolic link pointing to an arbitrary directory or file on the host via directory traversal ("../"). This flaw allows the container to read and write to arbitrary files on the host system.	2024-06-12	8.1	CVE-2024-5154
salesagility -- suitecrm	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in events response entry point allows for a SQL injection attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	2024-06-10	9.8	CVE-2024-36412
salesagility -- suitecrm	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, an unverified IFrame can be added some some inputs, which could allow for a cross-site scripting attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	2024-06-10	9	CVE-2024-36417
salesagility -- suitecrm	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in the `Alerts` controller. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	2024-06-10	8.8	CVE-2024-36408
salesagility -- suitecrm	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in Tree data entry point. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	2024-06-10	8.8	CVE-2024-36409
salesagility -- suitecrm	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in EmailUIAjax messages count controller. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	2024-06-10	8.8	CVE-2024-36410
salesagility -- suitecrm	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in EmailUIAjax displayView controller. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	2024-06-10	8.8	CVE-2024-36411
salesagility -- suitecrm	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in uploaded file verification in products allows for remote code execution. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	2024-06-10	8.8	CVE-2024-36415
salesagility -- suitecrm	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a deprecated v4 API example with no log rotation allows denial of service by logging excessive data. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	2024-06-10	7.5	CVE-2024-36416
salesagility-- SuiteCRM	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in connectors allows an authenticated user to perform a remote code execution attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	2024-06-10	8.5	CVE-2024-36418
SAP_SE--SAP Financial Consolidation	SAP Financial Consolidation allows data to enter a Web application through an untrusted source. These endpoints are exposed over the network and it allows the user to modify the content from the web site. On successful exploitation, an attacker can cause significant impact to confidentiality and integrity of the application.	2024-06-11	8.1	CVE-2024-37177
SAP_SE--SAP NetWeaver AS Java	Due to unrestricted access to the Meta Model Repository services in SAP NetWeaver AS Java, attackers can perform DoS attacks on the application, which	2024-06-11	7.5	CVE-2024-34688

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	may prevent legitimate users from accessing it. This can result in no impact on confidentiality and integrity but a high impact on the availability of the application.			
Schneider Electric--Easergy Studio	CWE-428: Unquoted search path or element vulnerability exists in Easergy Studio, which could cause privilege escalation when a valid user replaces a trusted file name on the system and reboots the machine.	2024-06-12	7.8	CVE-2024-2747
Schneider Electric--EcoStruxure IT Gateway	CWE-798: Use of hard-coded credentials vulnerability exists that could cause local privilege escalation when logged in as a non-administrative user.	2024-06-12	7.8	CVE-2024-0865
Schneider Electric--Sage 1410	CWE-787: Out-of-bounds Write vulnerability exists that could result in an authentication bypass when sending a malformed POST request and particular configuration parameters are set.	2024-06-12	9.8	CVE-2024-37036
Schneider Electric--Sage 1410	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could allow an authenticated user with access to the device's web interface to corrupt files and impact device functionality when sending a crafted HTTP request.	2024-06-12	8.1	CVE-2024-37037
Schneider Electric--Sage 1410	CWE-276: Incorrect Default Permissions vulnerability exists that could allow an authenticated user with access to the device's web interface to perform unauthorized file and firmware uploads when crafting custom web requests.	2024-06-12	7.5	CVE-2024-37038
seacms -- seacms	SeaCMS 12.9 has a file deletion vulnerability via admin_template.php.	2024-06-10	9.1	CVE-2024-31611
securenvoy -- multi-factor_authentication_solutions	Multiple LDAP injections vulnerabilities exist in SecurEnvoy MFA before 9.4.514 due to improper validation of user-supplied input. An unauthenticated remote attacker could exfiltrate data from Active Directory through blind LDAP injection attacks against the DESKTOP service exposed on the /secserver HTTP endpoint. This may include ms-Mcs-AdmPwd, which has a cleartext password for the Local Administrator Password Solution (LAPS) feature.	2024-06-10	7.5	CVE-2024-37393
Siemens--PowerSys	A vulnerability has been identified in PowerSys (All versions < V3.11). The affected application insufficiently protects responses to authentication requests. This could allow a local attacker to bypass authentication, thereby gaining administrative privileges for the managed remote devices.	2024-06-11	9.3	CVE-2024-36266
Siemens--SIMATIC S7-200 SMART CPU CR40	A vulnerability has been identified in SIMATIC S7-200 SMART CPU CR40 (6ES7288-1CR40-0AA0) (All versions), SIMATIC S7-200 SMART CPU CR60 (6ES7288-1CR60-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR20 (6ES7288-1SR20-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR20 (6ES7288-1SR20-0AA1) (All versions), SIMATIC S7-200 SMART CPU SR30 (6ES7288-1SR30-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR30 (6ES7288-1SR30-0AA1) (All versions), SIMATIC S7-200 SMART CPU SR40 (6ES7288-1SR40-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR40 (6ES7288-1SR40-0AA1) (All versions), SIMATIC S7-200 SMART CPU SR60 (6ES7288-1SR60-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR60 (6ES7288-1SR60-0AA1) (All versions), SIMATIC S7-200 SMART CPU ST20 (6ES7288-1ST20-0AA0) (All versions), SIMATIC S7-200 SMART CPU ST20 (6ES7288-1ST20-0AA1) (All versions), SIMATIC S7-200 SMART CPU ST30 (6ES7288-1ST30-0AA0) (All versions), SIMATIC S7-200 SMART CPU ST30 (6ES7288-1ST30-0AA1) (All versions), SIMATIC S7-200 SMART CPU ST40 (6ES7288-1ST40-0AA0) (All versions), SIMATIC S7-200 SMART CPU ST40 (6ES7288-1ST40-0AA1) (All versions), SIMATIC S7-200 SMART CPU ST60 (6ES7288-1ST60-0AA0) (All versions), SIMATIC S7-200 SMART CPU ST60 (6ES7288-1ST60-0AA1) (All versions). Affected devices are using a predictable IP ID sequence number. This leaves the system susceptible to a family of attacks which rely on the use of predictable IP ID sequence numbers as their base method of attack and eventually could allow an attacker to create a denial of service condition.	2024-06-11	8.2	CVE-2024-35292
Siemens--SINEC Traffic Analyzer	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V1.2). The affected application does not expire the session. This could allow an attacker to get unauthorized access.	2024-06-11	7.8	CVE-2024-35206
Siemens--SINEC Traffic Analyzer	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V1.2). The web interface of the affected devices are vulnerable to Cross-Site Request Forgery(CSRF) attacks. By tricking an authenticated victim user to click a malicious link, an attacker could perform arbitrary actions on the device on behalf of the victim user.	2024-06-11	7.8	CVE-2024-35207
Siemens--SINEC Traffic Analyzer	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V1.2). The affected web server is allowing HTTP methods like PUT and Delete. This could allow an attacker to modify unauthorized files.	2024-06-11	7.5	CVE-2024-35209

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Siemens--SINEC Traffic Analyzer	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V1.2). The affected application lacks input validation due to which an attacker can gain access to the Database entries.	2024-06-11	7.5	CVE-2024-35212
Siemens--Tecnomatix Plant Simulation V2302	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0012), Tecnomatix Plant Simulation V2404 (All versions < V2404.0001). The affected applications contain a type confusion vulnerability while parsing specially crafted MODEL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-22958)	2024-06-11	7.8	CVE-2024-35303
Soar Cloud--HR Portal	The notification emails sent by Soar Cloud HR Portal contain a link with a embedded session. The expiration of the session is not properly configured, remaining valid for more than 7 days and can be reused.	2024-06-14	8.8	CVE-2024-5995
Soar Cloud--HR Portal	The notification emails sent by Soar Cloud HR Portal contain a link with a embedded session. These emails are sent without using an encrypted transmission protocol. If an attacker intercepts the packets, they can obtain the plaintext session information and use it to log into the system.	2024-06-14	8.8	CVE-2024-5996
SourceCodester--Employee and Visitor Gate Pass Logging System	A vulnerability, which was classified as critical, was found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. Affected is the function save_users of the file /classes/Users.php?f=save. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-268140.	2024-06-12	7.3	CVE-2024-5896
SourceCodester--Employee and Visitor Gate Pass Logging System	A vulnerability was found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. It has been classified as critical. Affected is the function log_employee of the file /classes/Master.php?f=log_employee. The manipulation of the argument employee_code 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-268422 is the identifier assigned to this vulnerability.	2024-06-13	7.3	CVE-2024-5976
SourceCodester--Online Eyewear Shop	A vulnerability classified as critical was found in SourceCodester Online Eyewear Shop 1.0. This vulnerability affects unknown code of the file manage_product.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-268138 is the identifier assigned to this vulnerability.	2024-06-12	7.3	CVE-2024-5894
strapi--strapi	Strapi is an open-source content management system. By combining two vulnerabilities (an `Open Redirect` and `session token sent as URL query parameter`) in @strapi/plugin-users-permissions before version 4.24.2, is its possible of an unauthenticated attacker to bypass authentication mechanisms and retrieve the 3rd party tokens. The attack requires user interaction (one click). Unauthenticated attackers can leverage two vulnerabilities to obtain an 3rd party token and the bypass authentication of Strapi apps. Users should upgrade @strapi/plugin-users-permissions to version 4.24.2 to receive a patch.	2024-06-12	7.1	CVE-2024-34065
strategery-migrations_project -- strategery-migrations	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Gabriel Somoza / Joseph Fitzgibbons Strategery Migrations allows Path Traversal, File Manipulation.This issue affects Strategery Migrations: from n/a through 1.0.	2024-06-10	7.5	CVE-2024-35745
stylemixthemes -- mega_menu	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in StylemixThemes MegaMenu allows PHP Local File Inclusion.This issue affects MegaMenu: from n/a through 2.3.12.	2024-06-10	9.8	CVE-2024-35677
tagDiv--tagDiv Composer	The tagDiv Composer plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 4.8 via the 'td_block_title' shortcode 'block_template_id' attribute. This makes it possible for authenticated attackers, with contributor-level and above permissions, to include and execute arbitrary files 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 php file type can be uploaded and included.	2024-06-15	8.8	CVE-2024-3813
themehigh -- checkout_field_editor_for_woocommerce	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in ThemeHigh Checkout Field Editor for WooCommerce (Pro) allows Functionality Misuse, File Manipulation.This issue affects Checkout Field Editor for WooCommerce (Pro): from n/a through 3.6.2.	2024-06-10	9.1	CVE-2024-35658
themekraft -- buddypress_woocommerce_my_account_integration._create_woocomm	Missing Authorization vulnerability in ThemeKraft WooBuddy.This issue affects WooBuddy: from n/a through 3.4.19.	2024-06-10	8.8	CVE-2024-35726

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
erce_member_pages				
Themeum--Tutor LMS	Missing Authorization vulnerability in Themeum Tutor LMS.This issue affects Tutor LMS: from n/a through 2.1.8.	2024-06-11	8.3	CVE-2023-25799
tickera -- tickera	Missing Authorization vulnerability in Tickera.This issue affects Tickera: from n/a through 3.5.2.6.	2024-06-10	8.8	CVE-2024-35729
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	Toshiba printers use SNMP for configuration. Using the private community, it is possible to remotely execute commands as root on the remote printer. Using this vulnerability will allow any attacker to get a root access on a remote Toshiba printer. This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone.Â So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability.Â For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	2024-06-14	9.8	CVE-2024-27143
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	The Toshiba printers provide several ways to upload files using the web interface without authentication. An attacker can overwrite any insecure files. And the Toshiba printers are vulnerable to a Local Privilege Escalation vulnerability. An attacker can remotely compromise any Toshiba printer. The programs can be replaced by malicious programs by any local or remote attacker.Â This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone.Â So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability.Â For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	2024-06-14	9.8	CVE-2024-27144
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	The Toshiba printers provide several ways to upload files using the admin web interface. An attacker can remotely compromise any Toshiba printer. An attacker can overwrite any insecure files.Â This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone.Â So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability.Â For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	2024-06-14	9.8	CVE-2024-27145
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	Remote Command program allows an attacker to get Remote Code Execution. As for the affected products/models/versions, see the reference URL.	2024-06-14	9.8	CVE-2024-27172
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	Remote Command program allows an attacker to get Remote Code Execution by overwriting existing Python files containing executable code.Â This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone. So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability. For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	2024-06-14	9.8	CVE-2024-27173
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	Remote Command program allows an attacker to get Remote Code Execution. This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone. So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability. For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	2024-06-14	9.8	CVE-2024-27174
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	Toshiba printers provides API without authentication for internal access. A local attacker can bypass authentication in applications, providing administrative access. As for the affected products/models/versions, see the reference URL.	2024-06-14	8.4	CVE-2024-27169

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	Attackers can bypass the web login authentication process to gain access to the printer's system information and upload malicious drivers to the printer. As for the affected products/models/versions, see the reference URL.	2024-06-14	8.8	CVE-2024-3496
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	Path traversal vulnerability in the web server of the Toshiba printer enables attacker to overwrite orginal files or add new ones to the printer. As for the affected products/models/versions, see the reference URL.	2024-06-14	8.8	CVE-2024-3497
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	The Toshiba printers are vulnerable to a Local Privilege Escalation vulnerability. An attacker can remotely compromise any Toshiba printer. As for the affected products/models/versions, see the reference URL.	2024-06-14	7.4	CVE-2024-27147
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	The Toshiba printers are vulnerable to a Local Privilege Escalation vulnerability. An attacker can remotely compromise any Toshiba printer. As for the affected products/models/versions, see the reference URL.	2024-06-14	7.4	CVE-2024-27148
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	The Toshiba printers are vulnerable to a Local Privilege Escalation vulnerability. An attacker can remotely compromise any Toshiba printer. As for the affected products/models/versions, see the reference URL.	2024-06-14	7.4	CVE-2024-27149
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	The Toshiba printers are vulnerable to a Local Privilege Escalation vulnerability. An attacker can remotely compromise any Toshiba printer. As for the affected products/models/versions, see the reference URL.	2024-06-14	7.4	CVE-2024-27150
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	The Toshiba printers are vulnerable to a Local Privilege Escalation vulnerability. An attacker can remotely compromise any Toshiba printer. The programs can be replaced by malicious programs by any local or remote attacker. As for the affected products/models/versions, see the reference URL.	2024-06-14	7.4	CVE-2024-27151
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	The Toshiba printers are vulnerable to a Local Privilege Escalation vulnerability. An attacker can remotely compromise any Toshiba printer. As for the affected products/models/versions, see the reference URL.	2024-06-14	7.4	CVE-2024-27152
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	The Toshiba printers are vulnerable to a Local Privilege Escalation vulnerability. An attacker can remotely compromise any Toshiba printer. As for the affected products/models/versions, see the reference URL.	2024-06-14	7.4	CVE-2024-27153
Toshiba Tec Corporation--	The Toshiba printers are vulnerable to a Local Privilege Escalation vulnerability. An attacker can remotely compromise any Toshiba printer. The programs can be	2024-06-14	7.7	CVE-2024-27155

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Toshiba Tec e-Studio multi-function peripheral (MFP)	replaced by malicious programs by any local or remote attacker. As for the affected products/models/versions, see the reference URL.			
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	All the Toshiba printers share the same hardcoded root password. As for the affected products/models/versions, see the reference URL.	2024-06-14	7.4	CVE-2024-27158
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	Toshiba printers contain hardcoded credentials. As for the affected products/models/versions, see the reference URL.	2024-06-14	7.1	CVE-2024-27164
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	Toshiba printers contain a suidperl binary and it has a Local Privilege Escalation vulnerability. A local attacker can get root privileges. As for the affected products/models/versions, see the reference URL.	2024-06-14	7.8	CVE-2024-27165
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	Coredump binaries in Toshiba printers have incorrect permissions. A local attacker can steal confidential information. As for the affected products/models/versions, see the reference URL.	2024-06-14	7.4	CVE-2024-27166
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	Toshiba printers use Sendmail to send emails to recipients. Sendmail is used with several insecure directories. A local attacker can inject a malicious Sendmail configuration file. As for the affected products/models/versions, see the reference URL.	2024-06-14	7.4	CVE-2024-27167
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	It appears that some hardcoded keys are used for authentication to internal API. Knowing these private keys may allow attackers to bypass authentication and reach administrative interfaces. As for the affected products/models/versions, see the reference URL.	2024-06-14	7.1	CVE-2024-27168
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	It was observed that all the Toshiba printers contain credentials used for WebDAV access in the readable file. Then, it is possible to get a full access with WebDAV to the printer. As for the affected products/models/versions, see the reference URL.	2024-06-14	7.4	CVE-2024-27170
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	A remote attacker using the insecure upload functionality will be able to overwrite any Python file and get Remote Code Execution. As for the affected products/models/versions, see the reference URL.	2024-06-14	7.4	CVE-2024-27171
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-	An attacker can get Remote Code Execution by overwriting files. Overwriting files is enable by falsifying session ID variable. This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone. So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score"	2024-06-14	7.2	CVE-2024-27176

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
function peripheral (MFP)	of this vulnerability. For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.			
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	An attacker can get Remote Code Execution by overwriting files. Overwriting files is enable by falsifying package name variable. This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone. So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability. For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	2024-06-14	7.2	CVE-2024-27177
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	An attacker can get Remote Code Execution by overwriting files. Overwriting files is enable by falsifying file name variable. This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone. So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability. For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	2024-06-14	7.2	CVE-2024-27178
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	Attackers can then execute malicious files by enabling certain services of the printer via the web configuration page and elevate its privileges to root. As for the affected products/models/versions, see the reference URL.	2024-06-14	7.8	CVE-2024-3498
Trellix--Intrusion Prevention System (IPS) Manager	Insecure Deserialization in some workflows of the IPS Manager allows unauthenticated remote attackers to perform arbitrary code execution and access to the vulnerable Trellix IPS Manager.	2024-06-14	9.8	CVE-2024-5671
Trend Micro, Inc.--Trend Micro Apex One	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2024-36303.	2024-06-10	7.8	CVE-2024-36302
Trend Micro, Inc.--Trend Micro Apex One	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2024-36302.	2024-06-10	7.8	CVE-2024-36303
Trend Micro, Inc.--Trend Micro Apex One	A Time-of-Check Time-Of-Use vulnerability in the Trend Micro Apex One and Apex One as a Service agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2024-06-10	7.8	CVE-2024-36304
Trend Micro, Inc.--Trend Micro Apex One	A security agent link following vulnerability in Trend Micro Apex One could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2024-06-10	7.8	CVE-2024-36305
Trend Micro, Inc.--Trend Micro Apex One	An improper access control vulnerability in Trend Micro Apex One could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2024-06-10	7.8	CVE-2024-37289
Trend Micro, Inc.--Trend Micro Deep Security Agent	A link following vulnerability in Trend Micro Deep Security 20.x agents below build 20.0.1-3180 could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2024-06-10	7.8	CVE-2024-36358
Trend Micro, Inc.--Trend Micro Maximum Security (Consumer)	Trend Micro Security 17.x (Consumer) is vulnerable to a Privilege Escalation vulnerability that could allow a local attacker to unintentionally delete privileged Trend Micro files including its own.	2024-06-10	7.8	CVE-2024-32849
tribe29 -- checkmk	Improper restriction of excessive authentication attempts with two factor authentication methods in Checkmk 2.3 before 2.3.0p6 facilitates brute-forcing of second factor mechanisms.	2024-06-10	7.5	CVE-2024-28833
Verint--WFO	Verint - CWE-434: Unrestricted Upload of File with Dangerous Type	2024-06-13	8.8	CVE-2024-36396

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
webcraftic--Woody code snippets Insert Header Footer Code, AdSense Ads	The Woody code snippets - Insert Header Footer Code, AdSense Ads plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 2.5.0 via the 'insert_php' shortcode. This is due to the plugin not restricting the usage of the functionality to high level authorized users. This makes it possible for authenticated attackers, with contributor-level access and above, to execute code on the server.	2024-06-15	9.9	CVE-2024-3105
wedevs--Dokan Pro	The Dokan Pro plugin for WordPress is vulnerable to SQL Injection via the 'code' parameter in all versions up to, and including, 3.10.3 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.	2024-06-13	10	CVE-2024-3922
WPENGINE INC--Advanced Custom Fields PRO	Vulnerability discovered by executing a planned security audit. Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in WPENGINE INC Advanced Custom Fields PRO allows PHP Local File Inclusion.This issue affects Advanced Custom Fields PRO: from n/a before 6.2.10.	2024-06-10	9.9	CVE-2024-34762
WPENGINE INC--Advanced Custom Fields PRO	Vulnerability discovered by executing a planned security audit. Improper Control of Generation of Code ('Code Injection') vulnerability in WPENGINE INC Advanced Custom Fields PRO allows Code Injection.This issue affects Advanced Custom Fields PRO: from n/a before 6.2.10.	2024-06-10	8.5	CVE-2024-34761
wpmet--ElementsKit Pro	The ElementsKit PRO plugin for WordPress is vulnerable to Server-Side Request Forgery in versions up to, and including, 3.6.2 via the 'render_raw' function. This can allow authenticated attackers, with contributor-level permissions 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.	2024-06-14	8.5	CVE-2024-4404
WPStaging--WP STAGING Pro WordPress Backup Plugin	The WP STAGING Pro WordPress Backup Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 5.6.0. This is due to missing or incorrect nonce validation on the 'sub' parameter called from the WP STAGING WordPress Backup Plugin - Backup Duplicator & Migration plugin. This makes it possible for unauthenticated attackers to include any local files that end in '-settings.php' via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-06-14	7.5	CVE-2024-5551
WPWeb--WooCommerce - Social Login	The WooCommerce - Social Login plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 2.6.2 via deserialization of untrusted input from the 'woo_slg_verify' vulnerable parameter. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable software. 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.	2024-06-15	9.8	CVE-2024-5871
yotuwp--Video Gallery YouTube Playlist, Channel Gallery by YotuWP	The Video Gallery - YouTube Playlist, Channel Gallery by YotuWP plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.3.13 via the settings parameter. This makes it possible for unauthenticated attackers to include and execute arbitrary files 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.	2024-06-15	9.8	CVE-2024-4258
3uu--Shariff Wrapper	The Shariff Wrapper plugin for WordPress is vulnerable to Local File Inclusion in versions up to, and including, 4.6.13 via the shariff3uu_fetch_sharecounts function. This allows unauthenticated attackers to include and execute arbitrary files 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.	2024-06-20	9.8	CVE-2024-4098
Ali2Woo--Ali2Woo Lite	Cross-Site Request Forgery (CSRF) vulnerability in Ali2Woo Ali2Woo Lite.This issue affects Ali2Woo Lite: from n/a through 3.3.5.	2024-06-21	8.3	CVE-2024-37212
ali2woo--AliExpress Dropshipping with AliNext Lite	The AliExpress Dropshipping with AliNext Lite plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the ajax_save_image function in all versions up to, and including, 3.3.5. This makes it possible for authenticated attackers, with subscriber-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-06-19	8.8	CVE-2024-2381
AMD--AMD Ryzen Threadripper PRO Processors 5900	A potential weakness in AMD SPI protection features may allow a malicious attacker with Ring0 (kernel mode) access to bypass the native System Management Mode (SMM) ROM protections.	2024-06-18	8.2	CVE-2022-23829

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WX-Series				
Artbees--JupiterX Core	Incorrect Authorization vulnerability in Artbees JupiterX Core allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects JupiterX Core: from n/a through 3.3.8.	2024-06-21	9.8	CVE-2023-38389
Averta--Master Slider	Cross Site Scripting (XSS) vulnerability in Averta Master Slider allows Reflected XSS.This issue affects Master Slider: from n/a through 3.9.10.	2024-06-20	7.1	CVE-2024-37222
Bill Minozzi--WP Tools	Missing Authorization vulnerability in Bill Minozzi WP Tools.This issue affects WP Tools: from n/a through 3.41.	2024-06-21	8.8	CVE-2022-43453
Bogdan Bendziukov--Squeeze	Unrestricted Upload of File with Dangerous Type vulnerability in Bogdan Bendziukov Squeeze allows Code Injection.This issue affects Squeeze: from n/a through 1.4.	2024-06-21	9.1	CVE-2024-35767
Brainstorm Force--Convert Pro	Missing Authorization vulnerability in Brainstorm Force Convert Pro.This issue affects Convert Pro: from n/a through 1.7.5.	2024-06-19	7.1	CVE-2023-36684
Canonical Ltd.--snapd	When generating the systemd service units for the docker snap (and other similar snaps), snapd does not specify Delegate=yes - as a result systemd will move processes from the containers created and managed by these snaps into the cgroup of the main daemon within the snap itself when reloading system units. This may grant additional privileges to a container within the snap that were not originally intended.	2024-06-21	9.3	CVE-2020-27352
codevibrant--WP Blog Post Layouts	The WP Blog Post Layouts plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.1.3. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary PHP files 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.	2024-06-21	8.8	CVE-2024-5503
codevibrant--WP Magazine Modules Lite	The WP Magazine Modules Lite plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.1.2 via the 'blockLayout' parameter. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files 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.	2024-06-19	7.5	CVE-2024-5574
Crocoblock--JetElements For Elementor	Missing Authorization vulnerability in Crocoblock JetElements For Elementor.This issue affects JetElements For Elementor: from n/a through 2.6.13.	2024-06-19	8.2	CVE-2023-48760
Crocoblock--JetElements For Elementor	Missing Authorization vulnerability in Crocoblock JetElements For Elementor.This issue affects JetElements For Elementor: from n/a through 2.6.13.	2024-06-19	7.5	CVE-2023-48759
D-Link--G403	Certain models of D-Link wireless routers contain an undisclosed factory testing backdoor. Unauthenticated attackers on the local area network can force the device to enable Telnet service by accessing a specific URL and can log in by using the administrator credentials obtained from analyzing the firmware.	2024-06-17	8.8	CVE-2024-6045
deepjavalibrary--djl	DeepJavaLibrary(DJL) is an Engine-Agnostic Deep Learning Framework in Java. DJL versions 0.1.0 through 0.27.0 do not prevent absolute path archived artifacts from inserting archived files directly into the system, overwriting system files. This is fixed in DJL 0.28.0 and patched in DJL Large Model Inference containers version 0.27.0. Users are advised to upgrade.	2024-06-17	10	CVE-2024-37902
dglingren--Media Library Assistant	The Media Library Assistant plugin for WordPress is vulnerable to time-based SQL Injection via the 'order' parameter within the mla_tag_cloud Shortcode in all versions up to, and including, 3.16 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.	2024-06-20	8.8	CVE-2024-5605
dzikoysk--reposilite	Reposilite is an open source, lightweight and easy-to-use repository manager for Maven based artifacts in JVM ecosystem. Reposilite v3.5.10 is affected by an Arbitrary File Read vulnerability via path traversal while serving expanded javadoc	2024-06-19	8.6	CVE-2024-36117

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	files. Reposilite has addressed this issue in version 3.5.12. There are no known workarounds for this vulnerability. This issue was discovered and reported by the GitHub Security lab and is also tracked as GHSL-2024-074.			
dzikoysk--reposilite	Reposilite is an open source, lightweight and easy-to-use repository manager for Maven based artifacts in JVM ecosystem. As a Maven repository manager, Reposilite provides the ability to view the artifacts content in the browser, as well as perform administrative tasks via API. The problem lies in the fact that the artifact's content is served via the same origin (protocol/host/port) as the Admin UI. If the artifact contains HTML content with javascript inside, the javascript is executed within the same origin. Therefore, if an authenticated user is viewing the artifacts content, the javascript inside can access the browser's local storage where the user's password (aka 'token-secret') is stored. It is especially dangerous in scenarios where Reposilite is configured to mirror third party repositories, like the Maven Central Repository. Since anyone can publish an artifact to Maven Central under its own name, such malicious packages can be used to attack the Reposilite instance. This issue may lead to the full Reposilite instance compromise. If this attack is performed against the admin user, it's possible to use the admin API to modify settings and artifacts on the instance. In the worst case scenario, an attacker would be able to obtain the Remote code execution on all systems that use artifacts from Reposilite. It's important to note that the attacker does not need to lure a victim user to use a malicious artifact, but just open a link in the browser. This link can be silently loaded among the other HTML content, making this attack unnoticeable. Even if the Reposilite instance is located in an isolated environment, such as behind a VPN or in the local network, this attack is still possible as it can be performed from the admin browser. Reposilite has addressed this issue in version 3.5.12. Users are advised to upgrade. There are no known workarounds for this vulnerability. This issue was discovered and reported by the GitHub Security lab and is also tracked as GHSL-2024-072.	2024-06-19	7.1	CVE-2024-36115
dzikoysk--reposilite	Reposilite is an open source, lightweight and easy-to-use repository manager for Maven based artifacts in JVM ecosystem. Reposilite provides support for JavaDocs files, which are archives that contain documentation for artifacts. Specifically, JavadocEndpoints.kt controller allows to expand the javadoc archive into the server's file system and return its content. The problem is in the way how the archives are expanded, specifically how the new filename is created. The `file.name` taken from the archive can contain path traversal characters, such as '/../../../anything.txt', so the resulting extraction path can be outside the target directory. If the archive is taken from an untrusted source, such as Maven Central or JitPack for example, an attacker can craft a special archive to overwrite any local file on Reposilite instance. This could lead to remote code execution, for example by placing a new plugin into the '$workspace$/plugins' directory. Alternatively, an attacker can overwrite the content of any other package. Note that the attacker can use its own malicious package from Maven Central to overwrite any other package on Reposilite. Reposilite has addressed this issue in version 3.5.12. Users are advised to upgrade. There are no known workarounds for this vulnerability. This issue was discovered and reported by the GitHub Security lab and is also tracked as GHSL-2024-073.	2024-06-19	7.5	CVE-2024-36116
ESET, spol. s r.o.--ESET NOD32 Antivirus	Local privilege escalation vulnerability allowed an attacker to misuse ESET's file operations during a restore operation from quarantine.	2024-06-21	7.3	CVE-2024-2003
flipped-aurora--gin-vue-admin	Gin-vue-admin is a backstage management system based on vue and gin. Gin-vue-admin <= v2.6.5 has SQL injection vulnerability. The SQL injection vulnerabilities occur when a web application allows users to input data into SQL queries without sufficiently validating or sanitizing the input. Failing to properly enforce restrictions on user input could mean that even a basic form input field can be used to inject arbitrary and potentially dangerous SQL commands. This could lead to unauthorized access to the database, data leakage, data manipulation, or even complete compromise of the database server. This vulnerability has been addressed in commit `53d033821` which has been included in release version 2.6.6. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-06-17	8.8	CVE-2024-37896
Fortra--FileCatalyst Direct	A hard-coded password in the FileCatalyst TransferAgent can be found which can be used to unlock the keystore from which contents may be read out, for example, the private key for certificates. Exploit of this vulnerability could lead to a machine-in-the-middle (MiTM) attack against users of the agent. This issue affects all	2024-06-18	7.8	CVE-2024-5275

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	versions of FileCatalyst Direct from 3.8.10 Build 138 and earlier and all versions ofÃ, FileCatalyst Workflow from 5.1.6 Build 130 and earlier.			
GeoVision--GV_DSP_LPR_V2	Certain EOL GeoVision devices fail to properly filter user input for the specific functionality. Unauthenticated remote attackers can exploit this vulnerability to inject and execute arbitrary system commands on the device.	2024-06-17	9.8	CVE-2024-6047
GitHub--GitHub Enterprise Server	A Server-Side Request Forgery vulnerability was identified in GitHub Enterprise Server that allowed an attacker with the Site Administrator role to gain arbitrary code execution capability on the GitHub Enterprise Server instance. Exploitation required authenticated access to GitHub Enterprise Server as a user with the Site Administrator role.Ã, This vulnerability affected all versions of GitHub Enterprise Server prior to 3.13 and was fixed in versions 3.12.5, 3.11.11, 3.10.13, and 3.9.16. This vulnerability was reported via the GitHub Bug Bounty program.	2024-06-20	7.6	CVE-2024-5746
glboy--Login with phone number	The Login with phone number plugin for WordPress is vulnerable to unauthorized password resets in versions up to, and including 1.7.34. This is due to the plugin generating too weak a reset code, and the code used to reset the password has no attempt or time limit. This makes it possible for unauthenticated attackers to reset the password of arbitrary users by guessing a 6-digit numeric reset code.	2024-06-19	8.1	CVE-2024-6125
google -- chrome	Type Confusion in V8 in Google Chrome prior to 126.0.6478.114 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	2024-06-20	8.8	CVE-2024-6100
google -- chrome	Inappropriate implementation in V8 in Google Chrome prior to 126.0.6478.114 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	2024-06-20	8.8	CVE-2024-6101
google -- chrome	Out of bounds memory access in Dawn in Google Chrome prior to 126.0.6478.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-06-20	8.8	CVE-2024-6102
google -- chrome	Use after free in Dawn in Google Chrome prior to 126.0.6478.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-06-20	8.8	CVE-2024-6103
IBM--i	IBM i 7.3, 7.4, and 7.5 product IBM TCP/IP Connectivity Utilities for i contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain root access to the host operating system. IBM X-Force ID: 288171.	2024-06-21	7.8	CVE-2024-31890
IBM--QRadar Suite Software	IBM QRadar Suite Software 1.10.12.0 through 1.10.21.0 and IBM Cloud Pak for Security 1.10.12.0 through 1.10.21.0 could allow an authenticated user to execute certain arbitrary commands due to improper input validation. IBM X-Force ID: 272087.	2024-06-18	7.1	CVE-2023-47726
IBM--Security SOAR	IBM Security SOAR 51.0.2.0 could allow an authenticated user to execute malicious code loaded from a specially crafted script. IBM X-Force ID: 294830.	2024-06-22	7.5	CVE-2024-38319
IBM--Storage Protect for Virtual Environments: Data Protection for VMware	IBM Storage Protect for Virtual Environments: Data Protection for VMware 8.1.0.0 through 8.1.22.0 could allow a remote authenticated attacker to bypass security restrictions, caused by improper validation of user permission. By sending a specially crafted request, an attacker could exploit this vulnerability to change its settings, trigger backups, restore backups, and also delete all previous backups via log rotation. IBM X-Force ID: 294994.	2024-06-19	7.7	CVE-2024-38329
IBM--WebSphere Application Server	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to identity spoofing by an authenticated user due to improper signature validation. IBM X-Force ID: 294721.	2024-06-20	8.8	CVE-2024-37532
icegram--Email Subscribers by Icegram Express Email Marketing, Newsletters, Automation for WordPress & WooCommerce	The Email Subscribers by Icegram Express - Email Marketing, Newsletters, Automation for WordPress & WooCommerce plugin for WordPress is vulnerable to time-based SQL Injection via the db parameter in all versions up to, and including, 5.7.23 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.	2024-06-21	9.8	CVE-2024-5756
Intelbras--InControl	A vulnerability classified as critical was found in Intelbras InControl 2.21.56. This vulnerability affects unknown code. The manipulation leads to unquoted search path. Local access is required to approach this attack. The exploit has been	2024-06-17	7.8	CVE-2024-6080

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	disclosed to the public and may be used. VDB-268822 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure and plans to provide a solution within the next few weeks.			
itsourcecode--Bakery Online Ordering System	A vulnerability was found in itsourcecode Bakery Online Ordering System 1.0. It has been rated as critical. This issue affects some unknown processing of the file index.php. The manipulation of the argument user_email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-268793 was assigned to this vulnerability.	2024-06-17	7.3	CVE-2024-6065
itsourcecode--Banking Management System	A vulnerability was found in itsourcecode Banking Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file admin_class.php. The manipulation of the argument username 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-269168.	2024-06-20	7.3	CVE-2024-6196
itsourcecode--Farm Management System	A vulnerability was found in itsourcecode Farm Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file index.php of the component Login. The manipulation of the argument username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-269162 is the identifier assigned to this vulnerability.	2024-06-20	7.3	CVE-2024-6190
itsourcecode--Loan Management System	A vulnerability classified as critical was found in itsourcecode Loan Management System 1.0. This vulnerability affects unknown code of the file login.php of the component Login Page. The manipulation of the argument username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-269164.	2024-06-20	7.3	CVE-2024-6192
itsourcecode--Magbanua Beach Resort Online Reservation System	A vulnerability was found in itsourcecode Magbanua Beach Resort Online Reservation System up to 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file controller.php. The manipulation of the argument image 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-268856.	2024-06-18	7.3	CVE-2024-6110
itsourcecode--Monbela Tourist Inn Online Reservation System	A vulnerability was found in itsourcecode Monbela Tourist Inn Online Reservation System 1.0. It has been rated as critical. This issue affects some unknown processing of the file login.php. The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The identifier VDB-268865 was assigned to this vulnerability.	2024-06-20	7.3	CVE-2024-6113
itsourcecode--Monbela Tourist Inn Online Reservation System	A vulnerability classified as critical has been found in itsourcecode Monbela Tourist Inn Online Reservation System up to 1.0. Affected is an unknown function of the file controller.php. The manipulation of the argument image 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-268866 is the identifier assigned to this vulnerability.	2024-06-18	7.3	CVE-2024-6114
itsourcecode--Online Food Ordering System	A vulnerability was found in itsourcecode Online Food Ordering System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /purchase.php. The manipulation of the argument customer 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-269420.	2024-06-22	7.3	CVE-2024-6253
itsourcecode--Pool of Bethesda Online Reservation System	A vulnerability has been found in itsourcecode Pool of Bethesda Online Reservation System up to 1.0 and classified as critical. Affected by this vulnerability is the function uploadImage of the file /admin/mod_room/controller.php?action=add. The manipulation of the argument image leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-268825 was assigned to this vulnerability.	2024-06-18	7.3	CVE-2024-6084
itsourcecode--Pool of Bethesda Online Reservation System	A vulnerability classified as critical has been found in itsourcecode Pool of Bethesda Online Reservation System 1.0. This affects an unknown part of the file login.php. The manipulation of the argument email 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-268857 was assigned to this vulnerability.	2024-06-18	7.3	CVE-2024-6111
itsourcecode--Pool of Bethesda Online Reservation System	A vulnerability classified as critical was found in itsourcecode Pool of Bethesda Online Reservation System 1.0. This vulnerability affects unknown code of the file index.php. The manipulation of the argument log_email leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-268858 is the identifier assigned to this vulnerability.	2024-06-18	7.3	CVE-2024-6112
itsourcecode--Real Estate	A vulnerability was found in itsourcecode Real Estate Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of	2024-06-17	7.3	CVE-2024-6042

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management System	the file property-detail.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-268766 is the identifier assigned to this vulnerability.			
itsourcecode--Simple Online Hotel Reservation System	A vulnerability classified as critical was found in itsourcecode Simple Online Hotel Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the file add_room.php. The manipulation of the argument photo 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-268867.	2024-06-18	7.3	CVE-2024-6115
itsourcecode--Simple Online Hotel Reservation System	A vulnerability, which was classified as critical, has been found in itsourcecode Simple Online Hotel Reservation System 1.0. Affected by this issue is some unknown functionality of the file edit_room.php. The manipulation of the argument photo 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-268868.	2024-06-18	7.3	CVE-2024-6116
itsourcecode--Student Management System	A vulnerability classified as critical has been found in itsourcecode Student Management System 1.0. This affects an unknown part of the file login.php of the component Login Page. The manipulation of the argument user leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-269163.	2024-06-20	7.3	CVE-2024-6191
itsourcecode--Vehicle Management System	A vulnerability, which was classified as critical, has been found in itsourcecode Vehicle Management System 1.0. This issue affects some unknown processing of the file driverprofile.php. The manipulation of the argument driverid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-269165 was assigned to this vulnerability.	2024-06-20	7.3	CVE-2024-6193
itsourcecode--Vehicle Management System	A vulnerability, which was classified as critical, has been found in itsourcecode Vehicle Management System 1.0. Affected by this issue is some unknown functionality of the file busprofile.php. The manipulation of the argument busid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-269282 is the identifier assigned to this vulnerability.	2024-06-21	7.3	CVE-2024-6218
laurent22--joplin	Joplin is a free, open source note taking and to-do application. A Cross-site Scripting (XSS) vulnerability allows an untrusted note opened in safe mode to execute arbitrary code. `packages/renderer/MarkupToHtml.ts` renders note content in safe mode by surrounding it with <pre> and </pre>, without escaping any interior HTML tags. Thus, an attacker can create a note that closes the opening <pre> tag, then includes HTML that runs JavaScript. Because the rendered markdown iframe has the same origin as the toplevel document and is not sandboxed, any scripts running in the preview iframe can access the top variable and, thus, access the toplevel NodeJS `require` function. `require` can then be used to import modules like fs or child_process and run arbitrary commands. This issue has been addressed in version 2.12.9 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-06-21	8.2	CVE-2023-37898
laurent22--joplin	Joplin is a free, open source note taking and to-do application. A Cross-site Scripting (XSS) vulnerability allows pasting untrusted data into the rich text editor to execute arbitrary code. HTML pasted into the rich text editor is not sanitized (or not sanitized properly). As such, the `onload` attribute of pasted images can execute arbitrary code. Because the TinyMCE editor frame does not use the `sandbox` attribute, such scripts can access NodeJS's `require` through the `top` variable. From this, an attacker can run arbitrary commands. This issue has been addressed in version 2.12.10 and users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-06-21	8.2	CVE-2023-38506
laurent22--joplin	Joplin is a free, open source note taking and to-do application. A Cross site scripting (XSS) vulnerability in affected versions allows clicking on an untrusted image link to execute arbitrary shell commands. The HTML sanitizer (`packages/renderer/htmlUtils.ts::sanitizeHtml`) preserves `<map>` `<area>` links. However, unlike `<a>` links, the `target` and `href` attributes are not removed. Additionally, because the note preview pane isn't sandboxed to prevent top navigation, links with `target` set to `_top` can replace the toplevel electron page. Because any toplevel electron page, with Joplin's setup, has access to `require` and can require node libraries, a malicious replacement toplevel page can import `child_process` and execute arbitrary shell commands. This issue has been fixed in	2024-06-21	8.2	CVE-2023-39517

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	commit 7c52c3e9a81a52ef1b42a951f9deb9d378d59b0f which is included in release version 2.12.8. Users are advised to upgrade. There are no known workarounds for this vulnerability.			
laurent22--joplin	Joplin is a free, open source note taking and to-do application. A remote code execution (RCE) vulnerability in affected versions allows clicking on a link in a PDF in an untrusted note to execute arbitrary shell commands. Clicking links in PDFs allows for arbitrary code execution because Joplin desktop: 1. has not disabled top redirection for note viewer iframes, and 2. and has node integration enabled. This is a remote code execution vulnerability that impacts anyone who attaches untrusted PDFs to notes and has the icon enabled. This issue has been addressed in version 2.13.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-06-21	8.9	CVE-2023-45673
Live Composer Team--Page Builder: Live Composer	Deserialization of Untrusted Data vulnerability in Live Composer Team Page Builder: Live Composer.This issue affects Page Builder: Live Composer: from n/a through 1.5.42.	2024-06-19	8.5	CVE-2024-35780
mgibbs189--Custom Field Suite	The Custom Field Suite plugin for WordPress is vulnerable to SQL Injection via the the 'Term' custom field in all versions up to, and including, 2.6.7 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 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.	2024-06-20	8.8	CVE-2024-3561
mgibbs189--Custom Field Suite	The Custom Field Suite plugin for WordPress is vulnerable to PHP Code Injection in all versions up to, and including, 2.6.7 via the Loop custom field. This is due to insufficient sanitization of input prior to being used in a call to the eval() function. This makes it possible for authenticated attackers, with contributor-level access and above, to execute arbitrary PHP code on the server.	2024-06-20	8.8	CVE-2024-3562
Muffin Group--Betheme	Missing Authorization vulnerability in Muffin Group Betheme.This issue affects Betheme: from n/a through 27.1.1.	2024-06-19	7.6	CVE-2023-47770
Muffingroup--Betheme	Missing Authorization vulnerability in Muffingroup Betheme.This issue affects Betheme: from n/a through 27.1.1.	2024-06-19	8.2	CVE-2023-39998
n/a--opencart/opencart	This affects versions of the package opencart/opencart from 0.0.0. An SQL Injection issue was identified in the Divido payment extension for OpenCart, which is included by default in version 3.0.3.9. As an anonymous unauthenticated user, if the Divido payment module is installed (it does not have to be enabled), it is possible to exploit SQL injection to gain unauthorised access to the backend database. For any site which is vulnerable, any unauthenticated user could exploit this to dump the entire OpenCart database, including customer PII data.	2024-06-22	7.4	CVE-2024-21514
n/a--opencart/opencart	This affects versions of the package opencart/opencart from 4.0.0.0. A Zip Slip issue was identified via the marketplace installer due to improper sanitization of the target path, allowing files within a malicious archive to traverse the filesystem and be extracted to arbitrary locations. An attacker can create arbitrary files in the web root of the application and overwrite other existing files by exploiting this vulnerability.	2024-06-22	7.2	CVE-2024-21518
n/a--VMware vCenter Server	vCenter Server contains a heap-overflow vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger this vulnerability by sending a specially crafted network packet potentially leading to remote code execution.	2024-06-18	9.8	CVE-2024-37079
n/a--VMware vCenter Server	vCenter Server contains a heap-overflow vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger this vulnerability by sending a specially crafted network packet potentially leading to remote code execution.	2024-06-18	9.8	CVE-2024-37080
n/a--VMware vCenter Server	The vCenter Server contains multiple local privilege escalation vulnerabilities due to misconfiguration of sudo.Ã, An authenticated local user with non-administrative privileges may exploit these issues to elevate privileges to root on vCenter Server Appliance.	2024-06-18	7.8	CVE-2024-37081
nimble3--WordPress Picture / Portfolio / Media Gallery	The WordPress Picture / Portfolio / Media Gallery plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 3.0.1 via the 'file_get_contents' function. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web	2024-06-19	9.3	CVE-2024-5021

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	application and can be used to query and modify information from internal services.			
ollybach--WPPizza	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ollybach WPPizza allows Reflected XSS.This issue affects WPPizza: from n/a through 3.18.13.	2024-06-21	7.1	CVE-2024-35766
open-quantum-safe--oqs-provider	oqs-provider is a provider for the OpenSSL 3 cryptography library that adds support for post-quantum cryptography in TLS, X.509, and S/MIME using post-quantum algorithms from liboqs. Flaws have been identified in the way oqs-provider handles lengths decoded with DECODE_UINT32 at the start of serialized hybrid (traditional + post-quantum) keys and signatures. Unchecked length values are later used for memory reads and writes; malformed input can lead to crashes or information leakage. Handling of plain/non-hybrid PQ key operation is not affected. This issue has been patched in in v0.6.1. All users are advised to upgrade. There are no workarounds for this issue.	2024-06-17	8.2	CVE-2024-37305
Openfind--MailGates 5.0	Openfind's MailGates and MailAudit fail to properly filter user input when analyzing email attachments. An unauthenticated remote attacker can exploit this vulnerability to inject system commands and execute them on the remote server.	2024-06-17	9.8	CVE-2024-6048
Paid Memberships Pro--Paid Memberships Pro CCBill Gateway	Missing Authorization vulnerability in Paid Memberships Pro Paid Memberships Pro CCBill Gateway.This issue affects Paid Memberships Pro CCBill Gateway: from n/a through 0.3.	2024-06-19	8.2	CVE-2023-40608
Parallels--Parallels Desktop	Improper privilege management vulnerability in Parallels Desktop Software, which affects versions earlier than 19.3.0. An attacker could add malicious code in a script and populate the BASH_ENV environment variable with the path to the malicious script, executing on application startup. An attacker could exploit this vulnerability to escalate privileges on the system.	2024-06-21	7.7	CVE-2024-6240 cve-
POSIMYTH--Nexter	Missing Authorization vulnerability in POSIMYTH Nexter.This issue affects Nexter: from n/a through 2.0.3.	2024-06-19	7.6	CVE-2023-45658
provectus--kafka-ui	Kafka UI is an Open-Source Web UI for Apache Kafka Management. Kafka UI API allows users to connect to different Kafka brokers by specifying their network address and port. As a separate feature, it also provides the ability to monitor the performance of Kafka brokers by connecting to their JMX ports. JMX is based on the RMI protocol, so it is inherently susceptible to deserialization attacks. A potential attacker can exploit this feature by connecting Kafka UI backend to its own malicious broker. This vulnerability affects the deployments where one of the following occurs: 1. dynamic.config.enabled property is set in settings. It's not enabled by default, but it's suggested to be enabled in many tutorials for Kafka UI, including its own README.md. OR 2. an attacker has access to the Kafka cluster that is being connected to Kafka UI. In this scenario the attacker can exploit this vulnerability to expand their access and execute code on Kafka UI as well. Instead of setting up a legitimate JMX port, an attacker can create an RMI listener that returns a malicious serialized object for any RMI call. In the worst case it could lead to remote code execution as Kafka UI has the required gadget chains in its classpath. This issue may lead to post-auth remote code execution. This is particularly dangerous as Kafka-UI does not have authentication enabled by default. This issue has been addressed in version 0.7.2. All users are advised to upgrade. There are no known workarounds for this vulnerability. These issues were discovered and reported by the GitHub Security lab and is also tracked as GHSL-2023-230.	2024-06-19	8.1	CVE-2024-32030
raajtram--Pexels: Free Stock Photos	The Pexels: Free Stock Photos plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'pexels_fsp_images_options_validate' function in all versions up to, and including, 1.2.2. This makes it possible for authenticated attackers, with contributor-level and above permissions, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-06-19	8.8	CVE-2024-6132
recorp--Export WP Page to Static HTML/CSS	The Export WP Page to Static HTML/CSS plugin for WordPress is vulnerable to Open Redirect in all versions up to, and including, 2.2.2. This is due to insufficient validation on the redirect url supplied via the rc_exported_zip_file parameter. This makes it possible for unauthenticated attackers to redirect users to potentially malicious sites if they can successfully trick them into performing an action.	2024-06-20	7.1	CVE-2024-3597
Red Hat--Red Hat build of Apache Camel 4.0 for	A vulnerability was found in Undertow. URL-encoded request path information can be broken for concurrent requests on ajp-listener, causing the wrong path to be processed and resulting in a possible denial of service.	2024-06-20	7.5	CVE-2024-6162

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Spring Boot				
robosoft--Photo Gallery, Images, Slider in Rbs Image Gallery	The Photo Gallery, Images, Slider in Rbs Image Gallery plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.2.19. This is due to missing or incorrect nonce validation on the 'rbs_ajax_create_article' and 'rbs_ajax_reset_views' functions. This makes it possible for unauthenticated attackers to create new posts and reset gallery view counts via a forged request granted they can trick a Contributor+ level user into performing an action such as clicking on a link.	2024-06-19	8.8	CVE-2024-5343
Saturday Drive--Ninja Forms	Missing Authorization vulnerability in Saturday Drive Ninja Forms.This issue affects Ninja Forms: from n/a through 3.6.25.	2024-06-19	7.6	CVE-2023-38386
Saturday Drive--Ninja Forms	Missing Authorization vulnerability in Saturday Drive Ninja Forms.This issue affects Ninja Forms: from n/a through 3.6.25.	2024-06-19	7.6	CVE-2023-38393
ServMask--All-in-One WP Migration Box Extension	Missing Authorization vulnerability in ServMask All-in-One WP Migration Box Extension, ServMask All-in-One WP Migration OneDrive Extension, ServMask All-in-One WP Migration Dropbox Extension, ServMask All-in-One WP Migration Google Drive Extension.This issue affects All-in-One WP Migration Box Extension: from n/a through 1.53; All-in-One WP Migration OneDrive Extension: from n/a through 1.66; All-in-One WP Migration Dropbox Extension: from n/a through 3.75; All-in-One WP Migration Google Drive Extension: from n/a through 2.79.	2024-06-19	7.3	CVE-2023-40004
SevenSpark--UberMenu	The UberMenu plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.8.3. This is due to missing or incorrect nonce validation on the ubermenu_delete_all_item_settings and ubermenu_reset_settings functions. This makes it possible for unauthenticated attackers to delete and reset 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.	2024-06-22	7.2	CVE-2024-3593
sirv--Image Optimizer, Resizer and CDN Sirv	The Image Optimizer, Resizer and CDN - Sirv plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the sirv_upload_file_by_chanks AJAX action in all versions up to, and including, 7.2.6. This makes it possible for authenticated attackers, with Contributor-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-06-19	9.9	CVE-2024-5853
socketio--socket.io	Socket.IO is an open source, real-time, bidirectional, event-based, communication framework. A specially crafted Socket.IO packet can trigger an uncaught exception on the Socket.IO server, thus killing the Node.js process. This issue is fixed by commit `15af22fc22` which has been included in `socket.io@4.6.2` (released in May 2023). The fix was backported in the 2.x branch as well with commit `d30630ba10`. Users are advised to upgrade. Users unable to upgrade may attach a listener for the "error" event to catch these errors.	2024-06-19	7.3	CVE-2024-38355
SourceCodester--Best House Rental Management System	A vulnerability classified as critical has been found in SourceCodester Best House Rental Management System 1.0. This affects the function login of the file admin_class.php. The manipulation of the argument username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-268767.	2024-06-17	7.3	CVE-2024-6043
SourceCodester--Food Ordering Management System	A vulnerability was found in SourceCodester Food Ordering Management System up to 1.0. It has been classified as critical. This affects an unknown part of the file login.php of the component Login Panel. The manipulation of the argument username 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-269277 was assigned to this vulnerability.	2024-06-21	7.3	CVE-2024-6213
Spring by VMware Tanzu--Spring Cloud Skipper	Spring Cloud Data Flow is a microservices-based Streaming and Batch data processing in Cloud Foundry and Kubernetes. The Skipper server has the ability to receive upload package requests. However, due to improper sanitization for upload path, a malicious user who has access to skipper server api can use a crafted upload request to write arbitrary file to any location on file system, may even compromises the server.	2024-06-19	8.8	CVE-2024-22263
strategy11team--Business Directory Plugin Easy Listing Directories for WordPress	The Business Directory Plugin plugin for WordPress is vulnerable to CSV Injection in versions up to, and including, 6.4.3 via the class-csv-exporter.php file. This allows authenticated attackers, with author-level permissions and above, to embed untrusted input into CSV files exported by administrators, which can result in code execution when these files are downloaded and opened on a local system with a vulnerable configuration.	2024-06-18	7.4	CVE-2023-5527

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Tenda--A301	A vulnerability was found in Tenda A301 15.13.08.12. It has been classified as critical. Affected is the function fromSetWirelessRepeat of the file /goform/WifiExtraSet. The manipulation of the argument wpapsk_crypto leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-269160. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-20	8.8	CVE-2024-6189
ThemeFusion--Avada	Missing Authorization vulnerability in ThemeFusion Avada.This issue affects Avada: from n/a through 7.11.1.	2024-06-19	9.1	CVE-2023-39312
ThemePunch OHG--Essential Grid	Missing Authorization vulnerability in ThemePunch OHG Essential Grid.This issue affects Essential Grid: from n/a through 3.0.18.	2024-06-19	8.3	CVE-2023-47771
ThemePunch OHG--Slider Revolution	Missing Authorization vulnerability in ThemePunch OHG Slider Revolution.This issue affects Slider Revolution: from n/a before 6.7.0.	2024-06-19	7.1	CVE-2024-34444
Themify--Themify Ultra	Missing Authorization vulnerability in Themify Themify Ultra.This issue affects Themify Ultra: from n/a through 7.3.5.	2024-06-19	8.3	CVE-2023-46146
Themify--Themify Ultra	Missing Authorization vulnerability in Themify Themify Ultra.This issue affects Themify Ultra: from n/a through 7.3.5.	2024-06-19	8.8	CVE-2023-46148
themifyme--Themify WooCommerce Product Filter	The Themify - WooCommerce Product Filter plugin for WordPress is vulnerable to time-based SQL Injection via the 'conditions' parameter in all versions up to, and including, 1.4.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-06-21	9.8	CVE-2024-6027
ThimPress--LearnPress	Missing Authorization vulnerability in ThimPress LearnPress.This issue affects LearnPress: from n/a through 4.2.3.	2024-06-19	7.3	CVE-2023-36515
ThimPress--LearnPress	Missing Authorization vulnerability in ThimPress LearnPress.This issue affects LearnPress: from n/a through 4.2.3.	2024-06-19	7.6	CVE-2023-36516
thimpress--WP Hotel Booking	The WP Hotel Booking plugin for WordPress is vulnerable to SQL Injection via the 'room_type' parameter of the /wphb/v1/rooms/search-rooms REST API endpoint in all versions up to, and including, 2.1.0 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.	2024-06-20	10	CVE-2024-3605
Thrive Themes--Thrive Theme Builder	Missing Authorization vulnerability in Thrive Themes Thrive Theme Builder.This issue affects Thrive Theme Builder: from n/a before 3.24.0.	2024-06-19	8.3	CVE-2023-47783
Unknown--The Plus Addons for Elementor Page Builder	The Plus Addons for Elementor Page Builder plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 5.5.4 via the 'magazine_style' parameter within the Dynamic Smart Showcase widget. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files 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.	2024-06-21	8.8	CVE-2024-5455
vcita--Online Booking & Scheduling Calendar for WordPress by vcita	The Online Booking & Scheduling Calendar for WordPress by vcita plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wp_id' parameter in all versions up to, and including, 4.4.2 due to missing authorization checks on processAction function, as well as insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that will execute whenever a user accesses a wp-admin dashboard.	2024-06-22	7.2	CVE-2024-5791
webhuntinfotech--Photo Video Gallery Master	The Photo Video Gallery Master plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.5.3 via deserialization of untrusted input 'PVGM_all_photos_details' parameter. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software. If a POP chain is	2024-06-19	8.8	CVE-2024-5724

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			
webinnane--Lifeline Donation	The Lifeline Donation plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 1.2.6. This is due to insufficient verification on the user being supplied during the checkout through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email.	2024-06-20	9.8	CVE-2024-5432
websockets--ws	ws is an open source WebSocket client and server for Node.js. A request with a number of headers exceeding theserver.maxHeadersCount threshold could be used to crash a ws server. The vulnerability was fixed in ws@8.17.1 (e55e510) and backported to ws@7.5.10 (22c2876), ws@6.2.3 (eeb76d3), and ws@5.2.4 (4abd8f6). In vulnerable versions of ws, the issue can be mitigated in the following ways: 1. Reduce the maximum allowed length of the request headers using the --max-http-header-size=size and/or the maxHeaderSize options so that no more headers than the server.maxHeadersCount limit can be sent. 2. Set server.maxHeadersCount to 0 so that no limit is applied.	2024-06-17	7.5	CVE-2024-37890
Westermo--L210-F2G Lynx	An attacker may be able to cause a denial-of-service condition by sending many SSH packets repeatedly.	2024-06-20	7.5	CVE-2024-32943
Westermo--L210-F2G Lynx	An attacker may be able to cause a denial-of-service condition by sending many packets repeatedly.	2024-06-20	7.5	CVE-2024-35246
Woo--WooCommerce Warranty Requests	Missing Authorization vulnerability in Woo WooCommerce Warranty Requests.This issue affects WooCommerce Warranty Requests: from n/a through 2.1.9.	2024-06-19	8.1	CVE-2023-37870
WooCommerce--WooCommerce Stripe Payment Gateway	Missing Authorization vulnerability in WooCommerce WooCommerce Stripe Payment Gateway.This issue affects WooCommerce Stripe Payment Gateway: from n/a through 7.4.0.	2024-06-19	7.5	CVE-2023-35049
wordpresschef--Salon Booking System	The Salon booking system plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the SLN_Action_Ajax_ImportAssistants function along with missing authorization checks in all versions up to, and including, 10.2. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-06-19	9.8	CVE-2024-3229
xwiki--xwiki-platform	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. When an admin disables a user account, the user's profile is executed with the admin's rights. This allows a user to place malicious code in the user profile before getting an admin to disable the user account. To reproduce, as a user without script nor programming rights, edit the about section of your user profile and add `{{groovy}}services.logging.getLogger("attacker").error("Hello from Groovy!"){{/groovy}}`. As an admin, go to the user profile and click the "Disable this account" button. Then, reload the page. If the logs show `attacker - Hello from Groovy!` then the instance is vulnerable. This has been patched in XWiki 14.10.21, 15.5.5, 15.10.6 and 16.0.0. Users are advised to upgrade. There are no known workarounds for this vulnerability. ### Workarounds We're not aware of any workaround except upgrading. ### References * https://jira.xwiki.org/browse/XWIKI-21611 * https://github.com/xwiki/xwiki-platform/commit/f89c8f47fad6e5cc7e68c69a7e0acde07f5eed5a	2024-06-20	9	CVE-2024-37899
Yokogawa Electric Corporation--CENTUM CS 3000	DLL Hijacking vulnerability has been found in CENTUM CAMS Log server provided by Yokogawa Electric Corporation. If an attacker is somehow able to intrude into a computer that installed affected product or access to a shared folder, by replacing the DLL file with a tampered one, it is possible to execute arbitrary programs with the authority of the SYSTEM account. The affected products and versions are as follows: CENTUM CS 3000 R3.08.10 to R3.09.50 CENTUM VP R4.01.00 to R4.03.00, R5.01.00 to R5.04.20, R6.01.00 to R6.11.10.	2024-06-17	8.5	CVE-2024-5650
youzify--Youzify BuddyPress Community, User Profile, Social Network & Membership Plugin for	The Youzify - BuddyPress Community, User Profile, Social Network & Membership Plugin for WordPress plugin for WordPress is vulnerable to SQL Injection via the order_by shortcode attribute in all versions up to, and including, 1.2.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL	2024-06-20	9.8	CVE-2024-4742

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WordPress	queries into already existing queries that can be used to extract sensitive information from the database.			
ZTE--ZXHN H388X	There is an unauthorized access vulnerability in ZTE H388X. If H388X is caused by brute-force serial port cracking,attackers with common user permissions can use this vulnerability to obtain elevated permissions on the affected device by performing specific operations.	2024-06-20	7.1	CVE-2023-25646 psirt@zte.com.cn
access_management_specialist_project -- access_management_specialist	An issue in Shenzhen Weitillage Industrial Co., Ltd the access management specialist V6.62.51215 allows a remote attacker to obtain sensitive information.	2024-06-24	7.5	CVE-2024-37677
aimeos--ai-client-html	ai-client-html is an Aimeos e-commerce HTML client component. Debug information revealed sensitive information from environment variables in error log. This issue has been patched in versions 2024.04.7, 2023.10.15, 2022.10.13 and 2021.10.22.	2024-06-25	8.8	CVE-2024-38516
amazon -- freertos-plus-tcp	FreeRTOS-Plus-TCP is a lightweight TCP/IP stack for FreeRTOS. FreeRTOS-Plus-TCP versions 4.0.0 through 4.1.0 contain a buffer over-read issue in the DNS Response Parser when parsing domain names in a DNS response. A carefully crafted DNS response with domain name length value greater than the actual domain name length, could cause the parser to read beyond the DNS response buffer. This issue affects applications using DNS functionality of the FreeRTOS-Plus-TCP stack. Applications that do not use DNS functionality are not affected, even when the DNS functionality is enabled. This vulnerability has been patched in version 4.1.1.	2024-06-24	8.1	CVE-2024-38373
Arista Networks--Arista Wireless Access Points	This Advisory describes an issue that impacts Arista Wireless Access Points. Any entity with the ability to authenticate via SSH to an affected AP as the "config" user is able to cause a privilege escalation via spawning a bash shell. The SSH CLI session does not require high permissions to exploit this vulnerability, but the config password is required to establish the session. The spawned shell is able to obtain root privileges.	2024-06-27	8.4	CVE-2024-4578 psirt@arista.com
auto-featured-image_project -- auto-featured-image	The Auto Featured Image plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'create_post_attachment_from_url' function in all versions up to, and including, 1.2. This makes it possible for authenticated attackers, with contributor-level and above permissions, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-06-27	8.8	CVE-2024-6054
Avaya--IP Office	An improper input validation vulnerability was discovered in Avaya IP Office that could allow remote command or code execution via a specially crafted web request to the Web Control component. Affected versions include all versions prior to 11.1.3.1.	2024-06-25	10	CVE-2024-4196
Avaya--IP Office	An unrestricted file upload vulnerability in Avaya IP Office was discovered that could allow remote command or code execution via the One-X component. Affected versions include all versions prior to 11.1.3.1.	2024-06-25	9.9	CVE-2024-4197
ays-pro--Quiz Maker	The Quiz Maker plugin for WordPress is vulnerable to time-based SQL Injection via the 'ays_questions' parameter in all versions up to, and including, 6.5.8.3 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.	2024-06-25	9.8	CVE-2024-6028
Baicells--Snap Router	Use of Hard-coded Credentials vulnerability in Baicells Snap Router BaiCE_BMI on EP3011 (User Passwords modules) allows unauthorized access to the device.	2024-06-25	9.3	CVE-2023-6198 security@baicells.com
BC Security--Empire	BC Security Empire before 5.9.3 is vulnerable to a path traversal issue that can lead to remote code execution. A remote, unauthenticated attacker can exploit this vulnerability over HTTP by acting as a normal agent, completing all cryptographic handshakes, and then triggering an upload of payload data containing a malicious path.	2024-06-27	9.8	CVE-2024-6127
Brocade--Fabric OS	A vulnerability in the default configuration of the Simple Network Management Protocol (SNMP) feature of Brocade Fabric OS versions before v9.0.0 could allow an authenticated, remote attacker to read data from an affected device via SNMP. The vulnerability is due to hard-coded, default community string in the configuration file for the SNMP daemon. An attacker could exploit this vulnerability by using the static community string in SNMP version 1 queries to an affected device.	2024-06-26	8.1	CVE-2024-5460

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ChatGPTNextWeb--ChatGPT-Next-Web	NextChat is a cross-platform ChatGPT/Gemini UI. There is a Server-Side Request Forgery (SSRF) vulnerability due to a lack of validation of the `endpoint` GET parameter on the WebDav API endpoint. This SSRF can be used to perform arbitrary HTTPS request from the vulnerable instance (MKCOL, PUT and GET methods supported), or to target NextChat users and make them execute arbitrary JavaScript code in their browser. This vulnerability has been patched in version 2.12.4.	2024-06-28	7.4	CVE-2024-38514
CycloneDX--cyclonedx-core-java	The CycloneDX core module provides a model representation of the SBOM along with utilities to assist in creating, validating, and parsing SBOMs. Before deserializing CycloneDX Bill of Materials in XML format, _cyclonedx-core-java_ leverages XPath expressions to determine the schema version of the BOM. The `DocumentBuilderFactory` used to evaluate XPath expressions was not configured securely, making the library vulnerable to XML External Entity (XXE) injection. This vulnerability has been fixed in cyclonedx-core-java version 9.0.4.	2024-06-28	7.5	CVE-2024-38374
DataDog--dd-trace-cpp	dd-trace-cpp is the Datadog distributed tracing for C++. When the library fails to extract trace context due to malformed unicode, it logs the list of audited headers and their values using the `nlohmann` JSON library. However, due to the way the JSON library is invoked, it throws an uncaught exception, which results in a crash. This vulnerability has been patched in version 0.2.2.	2024-06-28	7.5	CVE-2024-38525
Dell--Integrated Dell Remote Access Controller 9	iDRAC9, versions prior to 7.00.00.172 for 14th Generation and 7.10.50.00 for 15th and 16th Generations, contains a session hijacking vulnerability in IPMI. A remote attacker could potentially exploit this vulnerability, leading to arbitrary code execution on the vulnerable application.	2024-06-29	7.6	CVE-2024-25943
Dell--PowerProtect DD	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 contain a buffer overflow vulnerability. A remote low privileged attacker could potentially exploit this vulnerability, leading to an application crash or execution of arbitrary code on the vulnerable application's underlying operating system with privileges of the vulnerable application.	2024-06-26	8.8	CVE-2024-29176
Dell--PowerProtect DD	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 contain an OS command injection vulnerability in an admin operation. A remote low privileged attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the system application's underlying OS with the privileges of the vulnerable application. Exploitation may lead to a system take over by an attacker.	2024-06-26	8.8	CVE-2024-37140
Elastic--Elastic Cloud Enterprise	It was identified that under certain specific preconditions, an API key that was originally created with a specific privileges could be subsequently used to create new API keys that have elevated privileges.	2024-06-28	8.1	CVE-2024-37282
flippercode--WP Maps Display Google Maps Perfectly with Ease	The WordPress Plugin for Google Maps - WP MAPS plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter of the 'put_wpgm' shortcode in all versions up to, and including, 4.6.1 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 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.	2024-06-29	8.8	CVE-2024-2386
Fortra--FileCatalyst Workflow	A SQL Injection vulnerability in Fortra FileCatalyst Workflow allows an attacker to modify application data. Likely impacts include creation of administrative users and deletion or modification of data in the application database. Data exfiltration via SQL injection is not possible using this vulnerability. Successful unauthenticated exploitation requires a Workflow system with anonymous access enabled, otherwise an authenticated user is required. This issue affects all versions of FileCatalyst Workflow from 5.1.6 Build 135 and earlier.	2024-06-25	9.8	CVE-2024-5276
gitlab -- gitlab	An issue was discovered in GitLab CE/EE affecting all versions starting from 15.8 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows an attacker to trigger a pipeline as another user under certain circumstances.	2024-06-27	8.8	CVE-2024-5655
gitlab -- gitlab	Improper authorization in global search in GitLab EE affecting all versions from 16.11 prior to 16.11.5 and 17.0 prior to 17.0.3 and 17.1 prior to 17.1.1 allows an attacker leak content of a private repository in a public project.	2024-06-27	7.5	CVE-2024-6323
goauthentik--authentik	authentik is an open-source Identity Provider that emphasizes flexibility and versatility. Authentik API-Access-Token mechanism can be exploited to gain admin user privileges. A successful exploit of the issue will result in a user gaining full admin access to the Authentik application, including resetting user passwords and more. This issue has been patched in version(s) 2024.2.4, 2024.4.2 and 2024.6.0.	2024-06-28	8.8	CVE-2024-37905

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
goauthentik--authentik	authentik is an open-source Identity Provider. Access restrictions assigned to an application were not checked when using the OAuth2 Device code flow. This could potentially allow users without the correct authorization to get OAuth tokens for an application and access it. This issue has been patched in version(s) 2024.6.0, 2024.2.4 and 2024.4.3.	2024-06-28	8.6	CVE-2024-38371
HashiCorp--Shared library	HashiCorp's go-getter library can be coerced into executing Git update on an existing maliciously modified Git Configuration, potentially leading to arbitrary code execution.	2024-06-25	8.4	CVE-2024-6257 security@hashicorp.com
Hewlett Packard Enterprise (HPE)--HPE Athonet Mobile Core	A security vulnerability has been identified in HPE Athonet Mobile Core software. The core application contains a code injection vulnerability where a threat actor could execute arbitrary commands with the privilege of the underlying container leading to complete takeover of the target system.	2024-06-25	7.5	CVE-2024-6206 security-alert@hpe.com
Hitachi Vantara--Pentaho Business Analytics Server	Hitachi Vantara Pentaho Business Analytics Server prior to versions 10.1.0.0 and 9.3.0.7, including 8.3.x allow a malicious URL to inject content into the Analyzer plugin interface.	2024-06-26	8.8	CVE-2024-28983
Hitachi Vantara--Pentaho Business Analytics Server	Hitachi Vantara Pentaho Business Analytics Server prior to versions 10.1.0.0 and 9.3.0.7, including 8.3.x allow a malicious URL to inject content into the Analyzer plugin interface.	2024-06-26	8.8	CVE-2024-28984
Hitachi Vantara--Pentaho Business Analytics Server	Hitachi Vantara Pentaho Business Analytics Server versions before 10.1.0.0 and 9.3.0.7, including 8.3.x do not correctly protect the ACL service endpoint of the Pentaho User Console against XML External Entity Reference.	2024-06-26	7.1	CVE-2024-28982
IBM--MQ	IBM MQ 9.3 LTS and 9.3 CD could allow an authenticated user to escalate their privileges under certain configurations due to incorrect privilege assignment. IBM X-Force ID: 289894.	2024-06-28	7.5	CVE-2024-31912
IBM--OpenBMC	IBM OpenBMC FW1050.00 through FW1050.10 BMCWeb HTTPS server component could disclose sensitive URI content to an unauthorized actor that bypasses authentication channels. IBM X-ForceID: 290026.	2024-06-27	7.5	CVE-2024-31916
IBM--Security Access Manager Docker	IBM Security Access Manager Docker 10.0.0.0 through 10.0.7.1 could allow a local user to obtain root access due to improper access controls. IBM X-Force ID: 254638.	2024-06-27	8.4	CVE-2023-30997
IBM--Security Access Manager Docker	IBM Security Access Manager Docker 10.0.0.0 through 10.0.7.1 could allow a local user to obtain root access due to improper access controls. IBM X-Force ID: 254649.	2024-06-27	8.4	CVE-2023-30998
IBM--Security Access Manager Docker	IBM Security Access Manager Docker 10.0.0.0 through 10.0.7.1, under certain configurations, could allow a user on the network to install malicious packages. IBM X-Force ID: 261197.	2024-06-27	7.5	CVE-2023-38370
Icegram--Email Subscribers & Newsletters	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Icegram Email Subscribers & Newsletters allows SQL Injection.This issue affects Email Subscribers & Newsletters: from n/a through 5.7.25.	2024-06-26	9.3	CVE-2024-37252
InstaWP Team--InstaWP Connect	Improper Control of Generation of Code ('Code Injection') vulnerability in InstaWP Team InstaWP Connect allows Code Injection.This issue affects InstaWP Connect: from n/a through 0.1.0.38.	2024-06-24	10	CVE-2024-37228
Intrado--911 Emergency Gateway (EGW)	Intrado 911 Emergency Gateway login form is vulnerable to an unauthenticated blind time-based SQL injection, which may allow an unauthenticated remote attacker to execute malicious code, exfiltrate data, or manipulate the database.	2024-06-26	10	CVE-2024-18399119a7d8-5eab-497f-8521-727c672e3725
itsourcecode--Online Food Ordering System	A vulnerability has been found in itsourcecode Online Food Ordering System up to 1.0 and classified as critical. This vulnerability affects unknown code of the file /addproduct.php. The manipulation of the argument photo leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-269806 is the identifier assigned to this vulnerability.	2024-06-27	7.3	CVE-2024-6373
itsourcecode--Pool of Bethesda Online Reservation System	A vulnerability, which was classified as critical, has been found in itsourcecode Pool of Bethesda Online Reservation System 1.0. Affected by this issue is some unknown functionality of the file controller.php. The manipulation of the argument rmtype_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-269804.	2024-06-27	7.3	CVE-2024-6371

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
itsourcecode--Simple Online Hotel Reservation System	A vulnerability was found in itsourcecode Simple Online Hotel Reservation System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file index.php. The manipulation of the argument username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-269620.	2024-06-25	7.3	CVE-2024-6308
j11g -- cruddiy	The CRUDDIY project is vulnerable to shell command injection via sending a crafted POST request to the application server. The exploitation risk is limited since CRUDDIY is meant to be launched locally. Nevertheless, a user with the project running on their computer might visit a website which would send such a malicious request to the locally launched server.	2024-06-24	7.8	CVE-2024-4748
Juniper Networks--Session Smart Router	An Authentication Bypass Using an Alternate Path or Channel vulnerability in Juniper Networks Session Smart Router or conductor running with a redundant peer allows a network based attacker to bypass authentication and take full control of the device. Only routers or conductors that are running in high-availability redundant configurations are affected by this vulnerability. No other Juniper Networks products or platforms are affected by this issue. This issue affects: Session Smart Router: * All versions before 5.6.15, * from 6.0 before 6.1.9-lts, * from 6.2 before 6.2.5-sts. Session Smart Conductor: * All versions before 5.6.15, * from 6.0 before 6.1.9-lts, * from 6.2 before 6.2.5-sts. WAN Assurance Router: * 6.0 versions before 6.1.9-lts, * 6.2 versions before 6.2.5-sts.	2024-06-27	10	CVE-2024-2973
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm: zynqmp_dpsub: Always register bridge We must always register the DRM bridge, since zynqmp_dp_hpd_work_func calls drm_bridge_hpd_notify, which in turn expects hpd_mutex to be initialized. We do this before zynqmp_dpsub_drm_init since that calls drm_bridge_attach. This fixes the following lockdep warning: [19.217084] ------------[cut here]------------ [19.227530] DEBUG_LOCKS_WARN_ON(lock->magic != lock) [19.227768] WARNING: CPU: 0 PID: 140 at kernel/locking/mutex.c:582 __mutex_lock+0x4bc/0x550 [19.241696] Modules linked in: [19.244937] CPU: 0 PID: 140 Comm: kworker/0:4 Not tainted 6.6.20+ #96 [19.252046] Hardware name: xlnx,zynqmp (DT) [19.256421] Workqueue: events zynqmp_dp_hpd_work_func [19.261795] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [19.269104] pc : __mutex_lock+0x4bc/0x550 [19.273364] lr : __mutex_lock+0x4bc/0x550 [19.277592] sp : ffffffc085c5bbe0 [19.281066] x29: ffffffc085c5bbe0 x28: 0000000000000000 x27: ffffff88009417f8 [19.288624] x26: ffffff8800941788 x25: ffffff8800020008 x24: ffffffc082aa3000 [19.296227] x23: ffffffc080d90e3c x22: 0000000000000002 x21: 0000000000000000 [19.303744] x20: 0000000000000000 x19: ffffff88002f5210 x18: 0000000000000000 [19.311295] x17: 6c707369642e3030 x16: 3030613464662072 x15: 0720072007200720 [19.318922] x14: 0000000000000000 x13: 284e4f5f4e524157 x12: 0000000000000001 [19.326442] x11: 0001ffc085c5b940 x10: 0001ff88003f388b x9 : 0001ff88003f3888 [19.334003] x8 : 0001ff88003f3888 x7 : 0000000000000000 x6 : 0000000000000000 [19.341537] x5 : 0000000000000000 x4 : 0000000000001668 x3 : 0000000000000000 [19.349054] x2 : 0000000000000000 x1 : 0000000000000000 x0 : ffffff88003f3880 [19.356581] Call trace: [19.359160] __mutex_lock+0x4bc/0x550 [19.363032] mutex_lock_nested+0x24/0x30 [19.367187] drm_bridge_hpd_notify+0x2c/0x6c [19.371698] zynqmp_dp_hpd_work_func+0x44/0x54 [19.376364] process_one_work+0x3ac/0x988 [19.380660] worker_thread+0x398/0x694 [19.384736] kthread+0x1bc/0x1c0 [19.388241] ret_from_fork+0x10/0x20 [19.392031] irq event stamp: 183 [19.395450] hardirqs last enabled at (183): [<ffffffc0800b9278>] finish_task_switch.isra.0+0xa8/0x2d4 [19.405140] hardirqs last disabled at (182): [<ffffffc081ad3754>] __schedule+0x714/0xd04 [19.413612] softirqs last enabled at (114): [<ffffffc080133de8>] srcu_invoke_callbacks+0x158/0x23c [19.423128] softirqs last disabled at (110): [<ffffffc080133de8>] srcu_invoke_callbacks+0x158/0x23c [19.432614] ---[end trace 0000000000000000]--- (cherry picked from commit 61ba791c4a7a09a370c45b70a81b8c7d4cf6b2ae)	2024-06-24	7.8	CVE-2024-38664
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: riscv: prevent pt_regs corruption for secondary idle threads Top of the kernel thread stack should be reserved for pt_regs. However this is not the case for the idle threads of the secondary boot harts. Their stacks overlap with their pt_regs, so both may get corrupted. Similar issue has been fixed for the primary hart, see c7cdd96eca28 ("riscv: prevent stack corruption by reserving task_pt_regs(p) early"). However that fix was not propagated to the secondary harts. The problem has been noticed in some CPU hotplug tests with V enabled. The function smp_callin stored several	2024-06-24	7.8	CVE-2024-38667

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	registers on stack, corrupting top of pt_regs structure including status field. As a result, kernel attempted to save or restore inexistent V context.			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix buffer size in gfx_v9_4_3_init_ cp_compute_microcode() and rlc_microcode() The function gfx_v9_4_3_init_microcode in gfx_v9_4_3.c was generating about potential truncation of output when using the snprintf function. The issue was due to the size of the buffer 'ucode_prefix' being too small to accommodate the maximum possible length of the string being written into it. The string being written is "amdgpu/%s_mec.bin" or "amdgpu/%s_rlc.bin", where %s is replaced by the value of 'chip_name'. The length of this string without the %s is 16 characters. The warning message indicated that 'chip_name' could be up to 29 characters long, resulting in a total of 45 characters, which exceeds the buffer size of 30 characters. To resolve this issue, the size of the 'ucode_prefix' buffer has been reduced from 30 to 15. This ensures that the maximum possible length of the string being written into the buffer will not exceed its size, thus preventing potential buffer overflow and truncation issues. Fixes the below with gcc W=1: drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c: In function 'gfx_v9_4_3_early_init': drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:379:52: warning: '%s' directive output may be truncated writing up to 29 bytes into a region of size 23 [-Wformat-truncation=] 379 | snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_rlc.bin", chip_name); | ^~ ..... 439 | r = gfx_v9_4_3_init_rlc_microcode(adev, ucode_prefix); | ~~~~~~~~~~~~ drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:379:9: note: 'snprintf' output between 16 and 45 bytes into a destination of size 30 379 | snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_rlc.bin", chip_name); | ^~~~~~~ drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:413:52: warning: '%s' directive output may be truncated writing up to 29 bytes into a region of size 23 [-Wformat-truncation=] 413 | snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_mec.bin", chip_name); | ^~ ..... 443 | r = gfx_v9_4_3_init_cp_compute_microcode(adev, ucode_prefix); | ~~~~~~~~~~~~ drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:413:9: note: 'snprintf' output between 16 and 45 bytes into a destination of size 30 413 | snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_mec.bin", chip_name); | ^~~~~~~	2024-06-24	7.8	CVE-2024-39291
Magarsus Consultancy--SSO (Single Sign On)	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), CWE - 200 - Exposure of Sensitive Information to an Unauthorized Actor, CWE - 522 - Insufficiently Protected Credentials vulnerability in Magarsus Consultancy SSO (Single Sign On) allows SQL Injection.This issue affects SSO (Single Sign On): from 1.0 before 1.1.	2024-06-26	9.8	CVE-2024-4228
Membership Software--WishList Member X	Improper Control of Generation of Code ('Code Injection') vulnerability in Membership Software WishList Member X allows Code Injection.This issue affects WishList Member X: from n/a before 3.26.7.	2024-06-24	9.9	CVE-2024-37109
Membership Software--WishList Member X	Improper Privilege Management vulnerability in Membership Software WishList Member X allows Privilege Escalation.This issue affects WishList Member X: from n/a before 3.26.7.	2024-06-24	8.8	CVE-2024-37107
Membership Software--WishList Member X	Missing Authorization vulnerability in Membership Software WishList Member X.This issue affects WishList Member X: from n/a before 3.26.7.	2024-06-24	7.5	CVE-2024-37111
Mia Technology Inc.--Mia-Med Health Aplication	Improper Restriction of Excessive Authentication Attempts vulnerability in Mia Technology Inc. Mia-Med Health Aplication allows Interface Manipulation.This issue affects Mia-Med Health Aplication: before 1.0.14.	2024-06-24	7.5	CVE-2024-5862
Microsoft-- Microsoft Power Platform	An authenticated attacker can exploit an Untrusted Search Path vulnerability in Microsoft Dataverse to execute code over a network.	2024-06-27	8	CVE-2024-35260
mitmproxy--pdoc	pdoc provides API Documentation for Python Projects. Documentation generated with `pdoc --math` linked to JavaScript files from polyfill.io. The polyfill.io CDN has been sold and now serves malicious code. This issue has been fixed in pdoc 14.5.1.	2024-06-26	7.2	CVE-2024-38526
modalweb-- Advanced File	The Advanced File Manager plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 5.2.4 via the	2024-06-29	7.5	CVE-2024-5598

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Manager	'fma_local_file_system' function. This makes it possible for unauthenticated attackers to extract sensitive data including backups or other sensitive information if the files have been moved to the built-in Trash folder.			
Moxa--OnCell G3150A-LTE Series	OnCell G3470A-LTE Series firmware versions v1.7.7 and prior have been identified as vulnerable due to a lack of neutralized inputs in IPSec configuration. An attacker could modify the intended commands sent to target functions, which could cause malicious users to execute unauthorized commands.	2024-06-25	7.1	CVE-2024-4639 psirt@moxa.com
Moxa--OnCell G3150A-LTE Series	OnCell G3470A-LTE Series firmware versions v1.7.7 and prior have been identified as vulnerable due to missing bounds checking on buffer operations. An attacker could write past the boundaries of allocated buffer regions in memory, causing a program crash.	2024-06-25	7.1	CVE-2024-4640 psirt@moxa.com
Moxa--OnCell G3470A-LTE Series	OnCell G3470A-LTE Series firmware versions v1.7.7 and prior have been identified as vulnerable due to a lack of neutralized inputs in the web key upload function. An attacker could modify the intended commands sent to target functions, which could cause malicious users to execute unauthorized commands.	2024-06-25	7.1	CVE-2024-4638 psirt@moxa.com
n/a--n/a	An issue was discovered in the Agent in Delinea Privilege Manager (formerly Thycotic Privilege Manager) before 12.0.1096 on Windows. Sometimes, a non-administrator user can copy a crafted DLL file to a temporary directory (used by .NET Shadow Copies) such that privilege escalation can occur if the core agent service loads that file.	2024-06-28	7	CVE-2024-39708
Next4Biz CRM & BPM Software--Business Process Manangement (BPM)	Improper Control of Generation of Code ('Code Injection') vulnerability in Next4Biz CRM & BPM Software Business Process Manangement (BPM) allows Remote Code Inclusion.This issue affects Business Process Manangement (BPM): from 6.6.4.4 before 6.6.4.5.	2024-06-24	9.8	CVE-2024-5683
omron -- nj101-1000_firmware	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration.	2024-06-24	7.5	CVE-2024-33687
pendulum-project--ntpd-rs	nptd-rs is a tool for synchronizing your computer's clock, implementing the NTP and NTS protocols. There is a missing limit for accepted NTS-KE connections. This allows an unauthenticated remote attacker to crash ntpd-rs when an NTS-KE server is configured. Non NTS-KE server configurations, such as the default ntpd-rs configuration, are unaffected. This vulnerability has been patched in version 1.1.3.	2024-06-28	7.5	CVE-2024-38528
pgadmin.org--pgAdmin 4	pgAdmin <= 8.8 has an installation Directory permission issue. Because of this issue, attackers can gain unauthorised access to the installation directory on the Debian or RHEL 8 platforms.	2024-06-25	7.4	CVE-2024-6238 f86ef6dc-4d3a-42ad-8f28-e6d5547a5007
Progress Software Corporation--WhatsUp Gold	In WhatsUp Gold versions released before 2023.1.3, a Remote Code Execution issue exists in Progress WhatsUp Gold. This vulnerability allows an unauthenticated attacker to achieve the RCE as a service account through NmApi.exe.	2024-06-25	9.8	CVE-2024-4883
Progress Software Corporation--WhatsUp Gold	In WhatsUp Gold versions released before 2023.1.3, an unauthenticated Remote Code Execution vulnerability in Progress WhatsUpGold. The Apm.UI.Areas.APM.Controllers.CommunityController allows execution of commands with iisapppool\nmconsole privileges.	2024-06-25	9.8	CVE-2024-4884
Progress Software Corporation--WhatsUp Gold	In WhatsUp Gold versions released before 2023.1.3, an unauthenticated Remote Code Execution vulnerability in Progress WhatsUpGold. The WhatsUp.ExportUtilities.Export.GetFileWithoutZip allows execution of commands with iisapppool\nmconsole privileges.	2024-06-25	9.8	CVE-2024-4885
Progress Software Corporation--WhatsUp Gold	In WhatsUp Gold versions released before 2023.1.3, an authenticated user with certain permissions can upload an arbitrary file and obtain RCE using Apm.UI.Areas.APM.Controllers.Api.Applications.AppProfileImportController.	2024-06-25	8.8	CVE-2024-5008
Progress Software Corporation--WhatsUp Gold	In WhatsUp Gold versions released before 2023.1.3, an Improper Access Control vulnerability in Wug.UI.Controllers.InstallController.SetAdminPassword allows local attackers to modify admin's password.	2024-06-25	8.4	CVE-2024-5009
Progress Software Corporation--WhatsUp Gold	In WhatsUp Gold versions released before 2023.1.3, there is a missing authentication vulnerability in WUGDataAccess.Credentials. This vulnerability allows unauthenticated attackers to disclose Windows Credentials stored in the product Credential Library.	2024-06-25	8.6	CVE-2024-5012
Progress Software Corporation--	In WhatsUp Gold versions released before 2023.1.3, a vulnerability exists in the TestController functionality. A specially crafted unauthenticated HTTP request can lead to a disclosure of sensitive information.	2024-06-25	7.5	CVE-2024-5010

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WhatsUp Gold				
Progress Software Corporation--WhatsUp Gold	In WhatsUp Gold versions released before 2023.1.3, an uncontrolled resource consumption vulnerability exists. A specially crafted unauthenticated HTTP request to the TestController Chart functionality can lead to denial of service.	2024-06-25	7.5	CVE-2024-5011
Progress Software Corporation--WhatsUp Gold	In WhatsUp Gold versions released before 2023.1.3, an unauthenticated Denial of Service vulnerability was identified. An unauthenticated attacker can put the application into the SetAdminPassword installation step, which renders the application non-accessible.	2024-06-25	7.5	CVE-2024-5013
Progress Software Corporation--WhatsUp Gold	In WhatsUp Gold versions released before 2023.1.3, a Server Side Request Forgery vulnerability exists in the GetASPReport feature. This allows any authenticated user to retrieve ASP reports from an HTML form.	2024-06-25	7.1	CVE-2024-5014
Progress Software Corporation--WhatsUp Gold	In WhatsUp Gold versions released before 2023.1.3, an authenticated SSRF vulnerability in Wug.UI.Areas.Wug.Controllers.SessionControler.Update allows a low privileged user to chain this SSRF with an Improper Access Control vulnerability. This can be used to escalate privileges to Admin.	2024-06-25	7.1	CVE-2024-5015
Progress Software Corporation--WhatsUp Gold	In WhatsUp Gold versions released before 2023.1.3, Distributed Edition installations can be exploited by using a deserialization tool to achieve a Remote Code Execution as SYSTEM. The vulnerability exists in the main message processing routines NmDistributed.DistributedServiceBehavior.OnMessage for server and NmDistributed.DistributedClient.OnMessage for clients.	2024-06-25	7.2	CVE-2024-5016
Progress--MOVEit Gateway	Improper Authentication vulnerability in Progress MOVEit Gateway (SFTP modules) allows Authentication Bypass.This issue affects MOVEit Gateway: 2024.0.0.	2024-06-25	9.1	CVE-2024-5805
Progress--MOVEit Transfer	Improper Authentication vulnerability in Progress MOVEit Transfer (SFTP module) can lead to Authentication Bypass.This issue affects MOVEit Transfer: from 2023.0.0 before 2023.0.11, from 2023.1.0 before 2023.1.6, from 2024.0.0 before 2024.0.2.	2024-06-25	9.1	CVE-2024-5806
PTC--Creo Elements/Direct License	PTC Creo Elements/Direct License Server exposes a web interface which can be used by unauthenticated remote attackers to execute arbitrary OS commands on the server.	2024-06-27	10	CVE-2024-6071
renesas -- rcar_gen3	Incorrect Calculation vulnerability in Renesas arm-trusted-firmware allows Local Execution of Code. When checking whether a new image invades/overlaps with a previously loaded image the code neglects to consider a few cases. that could An attacker to bypass memory range restriction and overwrite an already loaded image partly or completely, which could result in code execution and bypass of secure boot.	2024-06-24	7.8	CVE-2024-6287
Salon Booking System--Salon booking system	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Salon Booking System Salon booking system allows File Manipulation.This issue affects Salon booking system: from n/a through 9.9.	2024-06-24	8.6	CVE-2024-37231
scidsg--hushline	Hush Line is a free and open-source, anonymous-tip-line-as-a-service for organizations or individuals. There is a stored XSS in the Inbox. The input is displayed using the `safe` Jinja2 attribute, and thus not sanitized upon display. This issue has been patched in version 0.1.0.	2024-06-28	8.8	CVE-2024-38521
scidsg--hushline	Hush Line is a free and open-source, anonymous-tip-line-as-a-service for organizations or individuals. The TOTP authentication flow has multiple issues that weakens its one-time nature. Specifically, the lack of 2FA for changing security settings allows attacker with CSRF or XSS primitives to change such settings without user interaction and credentials are required. This vulnerability has been patched in version 0.10.	2024-06-27	7.5	CVE-2024-38523
silabs.com--Ember ZNet SDK	An unauthenticated IEEE 802.15.4 'co-ordinator realignment' packet can be used to force Zigbee nodes to change their network identifier (pan ID), leading to a denial of service. This packet type is not useful in production and should be used only for PHY qualification.	2024-06-27	7.5	CVE-2024-3043
SoftEtherVPN--SoftEtherVPN	SoftEtherVPN is a an open-source cross-platform multi-protocol VPN Program. When SoftEtherVPN is deployed with L2TP enabled on a device, it introduces the possibility of the host being used for amplification/reflection traffic generation because it will respond to every packet with two response packets that are larger than the request packet size. These sorts of techniques are used by external actors who generate spoofed source IPs to target a destination on the internet. This vulnerability has been patched in version 5.02.5185.	2024-06-26	7.5	CVE-2024-38520

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Spotfire--Spotfire Analyst	Vulnerability in Spotfire Spotfire Analyst, Spotfire Spotfire Server, Spotfire Spotfire for AWS Marketplace allows In the case of the installed Windows client: Successful execution of this vulnerability will result in an attacker being able to run arbitrary code.This requires human interaction from a person other than the attacker., In the case of the Web player (Business Author): Successful execution of this vulnerability via the Web Player, will result in the attacker being able to run arbitrary code as the account running the Web player process, In the case of Automation Services: Successful execution of this vulnerability will result in an attacker being able to run arbitrary code via Automation Services..This issue affects Spotfire Analyst: from 12.0.9 through 12.5.0, from 14.0 through 14.0.2; Spotfire Server: from 12.0.10 through 12.5.0, from 14.0 through 14.0.3, from 14.2.0 through 14.3.0; Spotfire for AWS Marketplace: from 14.0 before 14.3.0.	2024-06-27	9.9	CVE-2024-3330 security@tibco.com
stiofansisland--UsersWP Front-end login form, User Registration, User Profile & Members Directory plugin for WordPress	The UsersWP - Front-end login form, User Registration, User Profile & Members Directory plugin for WordPress plugin for WordPress is vulnerable to time-based SQL Injection via the 'uwp_sort_by' parameter in all versions up to, and including, 1.2.10 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-06-29	9.8	CVE-2024-6265
StylemixThemes--Consulting Elementor Widgets	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in StylemixThemes Consulting Elementor Widgets allows PHP Local File Inclusion.This issue affects Consulting Elementor Widgets: from n/a through 1.3.0.	2024-06-24	9	CVE-2024-37089
StylemixThemes--Consulting Elementor Widgets	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in StylemixThemes Consulting Elementor Widgets allows OS Command Injection.This issue affects Consulting Elementor Widgets: from n/a through 1.3.0.	2024-06-24	9.9	CVE-2024-37091
StylemixThemes--Consulting Elementor Widgets	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in StylemixThemes Consulting Elementor Widgets allows PHP Local File Inclusion.This issue affects Consulting Elementor Widgets: from n/a through 1.3.0.	2024-06-24	8.5	CVE-2024-37092
Synology--Camera Firmware	A vulnerability regarding buffer copy without checking size of input ('Classic Buffer Overflow') is found in the libjansson component and it does not affect the upstream library. This allows remote attackers to execute arbitrary code via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.7-0298 may be affected: BC500 and TC500.	2024-06-28	9.8	CVE-2024-39349
Synology--Camera Firmware	A vulnerability regarding improper neutralization of special elements used in an OS command ('OS Command Injection') is found in the IP block functionality. This allows remote authenticated users with administrator privileges to execute arbitrary commands via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.7-0298 may be affected: BC500 and TC500.	2024-06-28	7.2	CVE-2023-47802
Synology--Camera Firmware	A vulnerability regarding authentication bypass by spoofing is found in the RTSP functionality. This allows man-in-the-middle attackers to obtain privileges without consent via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.7-0298 may be affected: BC500 and TC500.	2024-06-28	7.5	CVE-2024-39350
Synology--Camera Firmware	A vulnerability regarding improper neutralization of special elements used in an OS command ('OS Command Injection') is found in the NTP configuration. This allows remote authenticated users with administrator privileges to execute arbitrary commands via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.7-0298 may be affected: BC500 and TC500.	2024-06-28	7.2	CVE-2024-39351
Synology--Synology Router Manager (SRM)	Download of code without integrity check vulnerability in AirPrint functionality in Synology Router Manager (SRM) before 1.2.5-8227-11 and 1.3.1-9346-8 allows man-in-the-middle attackers to execute arbitrary code via unspecified vectors.	2024-06-28	7.5	CVE-2024-39348
Talya Informatics--Elektraweb	Reliance on Cookies without Validation and Integrity Checking vulnerability in Talya Informatics Elektraweb allows Session Credential Falsification through Manipulation, Accessing/Intercepting/Modifying HTTP Cookies, Manipulating Opaque Client-based Data Tokens.This issue affects Elektraweb: before v17.0.68.	2024-06-27	9.8	CVE-2024-0947
Talya Informatics--Elektraweb	Improper Access Control, Missing Authorization, Incorrect Authorization, Incorrect Permission Assignment for Critical Resource, Missing Authentication, Weak Authentication, Improper Restriction of Communication Channel to Intended Endpoints vulnerability in Talya Informatics Elektraweb allows Exploiting Incorrectly Configured Access Control Security Levels, Manipulating Web Input to	2024-06-27	9.8	CVE-2024-0949

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	File System Calls, Embedding Scripts within Scripts, Malicious Logic Insertion, Modification of Windows Service Configuration, Malicious Root Certificate, Intent Spoof, WebView Exposure, Data Injected During Configuration, Incomplete Data Deletion in a Multi-Tenant Environment, Install New Service, Modify Existing Service, Install Rootkit, Replace File Extension Handlers, Replace Trusted Executable, Modify Shared File, Add Malicious File to Shared Webroot, Run Software at Logon, Disable Security Software.This issue affects Elektraweb: before v17.0.68.			
Talya Informatics--Travel APPS	Authorization Bypass Through User-Controlled Key vulnerability in Talya Informatics Travel APPS allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Travel APPS: before v17.0.68.	2024-06-27	8.8	CVE-2024-1107
The Conduit Contributors--Conduit	Missing authorization in Client-Server API in Conduit <=0.7.0, allowing for any alias to be removed and added to another room, which can be used for privilege escalation by moving the #admins alias to a room which they control, allowing them to run commands resetting passwords, siging json with the server's key, deactivating users, and more	2024-06-25	9.9	CVE-2024-6303
The Conduit Contributors--Conduit	Lack of privilege checking when processing a redaction in Conduit versions v0.6.0 and lower, allowing a local user to redact any message from users on the same server, given that they are able to send redaction events.	2024-06-25	8.1	CVE-2024-6302
themewinter--WPCafe Online Food Ordering, Restaurant Menu, Delivery, and Reservations for WooCommerce	The WPCafe - Online Food Ordering, Restaurant Menu, Delivery, and Reservations for WooCommerce plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.2.25 via the reservation_extra_field shortcode parameter. This makes it possible for authenticated attackers, with Contributor-level access and above, to include remote files on the server, potentially resulting in code execution	2024-06-25	8.8	CVE-2024-5431
Tp-Link--ER7206 Omada Gigabit VPN Router	A leftover debug code vulnerability exists in the cli_server debug functionality of Tp-Link ER7206 Omada Gigabit VPN Router 1.4.1 Build 20240117 Rel.57421. A specially crafted series of network requests can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability.	2024-06-25	7.2	CVE-2024-21827
tpm2-software--tpm2-tools	tpm2 is the source repository for the Trusted Platform Module (TPM2.0) tools. This vulnerability allows attackers to manipulate tpm2_checkquote outputs by altering the TPML_PCR_SELECTION in the PCR input file. As a result, digest values are incorrectly mapped to PCR slots and banks, providing a misleading picture of the TPM state. This issue has been patched in version 5.7.	2024-06-28	9	CVE-2024-29039
usbarmory--mxs-dcp	The NXP Data Co-Processor (DCP) is a built-in hardware module for specific NXP SoCsÂ¹ that implements a dedicated AES cryptographic engine for encryption/decryption operations. The dcp_tool reference implementation included in the repository selected the test key, regardless of its `-t` argument. This issue has been patched in commit 26a7.	2024-06-28	7.1	CVE-2024-38532
virtosoftware --sharepoint_bulk_file_download	An issue was discovered in VirtoSoftware Virto Bulk File Download 5.5.44 for SharePoint 2019. The Virto.SharePoint.FileDownloader/Api/Download.ashx isCompleted method allows arbitrary file download and deletion via absolute path traversal in the path parameter.	2024-06-24	9.8	CVE-2024-33879
VMware--Salt Project	A specially crafted url can be created which leads to a directory traversal in the salt file server. A malicious user can read an arbitrary file from a Salt master's filesystem.	2024-06-27	7.7	CVE-2024-22232
warfareplugins--Social Sharing Plugin Social Warfare	Several plugins for WordPress hosted on WordPress.org have been compromised and injected with malicious PHP scripts. A malicious threat actor compromised the source code of various plugins and injected code that exfiltrates database credentials and is used to create new, malicious, administrator users and send that data back to a server. Currently, not all plugins have been patched and we strongly recommend uninstalling the plugins for the time being and running a complete malware scan.	2024-06-25	10	CVE-2024-6297
wpeka-club--Cookie Consent for WP Cookie Consent, Consent Log, Cookie Scanner, Script	The WP Cookie Consent (for GDPR, CCPA & ePrivacy) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Client-IP' header in all versions up to, and including, 3.2.0 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.	2024-06-26	7.2	CVE-2024-4869

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Blocker (for GDPR, CCPA & ePrivacy)				

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ninjateam--GDPR CCPA Compliance & Cookie Consent Banner	The GDPR CCPA Compliance & Cookie Consent Banner plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on several functions named ajaxUpdateSettings() in all versions up to, and including, 2.7.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify the plugin's settings, update page content, send arbitrary emails and inject malicious web scripts.	2024-06-07	5.4	CVE-2024-5607
10up--ElasticPress	Cross-Site Request Forgery (CSRF) vulnerability in 10up ElasticPress.This issue affects ElasticPress: from n/a through 5.1.0.	2024-06-08	4.3	CVE-2024-35684
10up--Restricted Site Access	Authentication Bypass by Spoofing vulnerability in 10up Restricted Site Access allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Restricted Site Access: from n/a through 7.4.1.	2024-06-04	5.3	CVE-2023-48753
10Web Form Builder Team--Form Maker by 10Web	Improper Restriction of Excessive Authentication Attempts vulnerability in 10Web Form Builder Team Form Maker by 10Web allows Functionality Bypass.This issue affects Form Maker by 10Web: from n/a through 1.15.20.	2024-06-04	5.3	CVE-2023-48290
10web--Photo Gallery by 10Web Mobile-Friendly Image Gallery	The Photo Gallery by 10Web - Mobile-Friendly Image Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'svg' parameter in all versions up to, and including, 1.8.23 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. By default, this can only be exploited by administrators, but the ability to use and configure Photo Gallery can be extended to contributors on pro versions of the plugin.	2024-06-07	6.4	CVE-2024-5426
10web--Photo Gallery by 10Web Mobile-Friendly	The Photo Gallery by 10Web - Mobile-Friendly Image Gallery plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.8.23 via the esc_dir function. This makes it possible for authenticated attackers to cut and paste (copy) the contents of arbitrary files on the server, which can contain sensitive information, and to cut (delete) arbitrary directories, including the root	2024-06-07	6.8	CVE-2024-5481

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Image Gallery	WordPress directory. By default this can be exploited by administrators only. In the premium version of the plugin, administrators can give gallery edit permissions to lower level users, which might make this exploitable by users as low as contributors.			
A WP Life--Contact Form Widget	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in A WP Life Contact Form Widget.This issue affects Contact Form Widget: from n/a through 1.3.9.	2024-06-03	5.3	CVE-2024-34754
AccessAlly--PopupAlly	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in AccessAlly PopupAlly allows Stored XSS.This issue affects PopupAlly: from n/a through 2.1.1.	2024-06-03	5.9	CVE-2024-34796
adamskaat--Countdown, Coming Soon, Maintenance Countdown & Clock	The Countdown, Coming Soon, Maintenance - Countdown & Clock plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the conditionsRow and switchCountdown functions in all versions up to, and including, 2.7.8. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject PHP Objects and modify the status of countdowns.	2024-06-06	5.4	CVE-2024-2017
Analytify--Analytify	Cross-Site Request Forgery (CSRF) vulnerability in Analytify.This issue affects Analytify: from n/a through 5.2.3.	2024-06-08	5.4	CVE-2024-35689
apollo13themes--Rife Free	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in apollo13themes Rife Free allows Stored XSS.This issue affects Rife Free: from n/a through 2.4.19.	2024-06-08	6.5	CVE-2024-35708
argoproj--argo-cd	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. The vulnerability allows unauthorized access to the sensitive settings exposed by /api/v1/settings endpoint without authentication. All sensitive settings are hidden except passwordPattern. This vulnerability is fixed in 2.11.3, 2.10.12, and 2.9.17.	2024-06-06	5.3	CVE-2024-37152
argoproj--argo-cd	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. It's possible for authenticated users to enumerate clusters by name by inspecting error messages. It's also possible to enumerate the names of projects with project-scoped clusters if you know the names of the clusters. This vulnerability is fixed in 2.11.3, 2.10.12, and 2.9.17.	2024-06-06	4.3	CVE-2024-36106
ARI Soft--ARI Stream Quiz	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in ARI Soft ARI Stream Quiz allows Code Injection.This issue affects ARI Stream Quiz: from n/a through 1.3.2.	2024-06-04	5.4	CVE-2023-47513
artbees--SellKit Funnel builder and checkout optimizer for WooCommerce to sell more, faster	The SellKit - Funnel builder and checkout optimizer for WooCommerce to sell more, faster plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter in all versions up to, and including, 1.9.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-06	6.4	CVE-2024-4608
Automattic--ChaosTheory	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Automattic ChaosTheory allows Stored XSS.This issue affects ChaosTheory: from n/a through 1.3.	2024-06-03	6.5	CVE-2024-34766
awordpresslife--Formula	The Formula theme for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'id' parameter in the 'quality_customizer_notify_dismiss_action' AJAX action in all versions up to, and including, 0.5.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-06-08	6.1	CVE-2024-5613

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
awordpresslife--Formula	The Formula theme for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'id' parameter in the 'ti_customizer_notify_dismiss_recommended_plugins' AJAX action in all versions up to, and including, 0.5.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-06-08	6.1	CVE-2024-5638
bdthemes--Prime Slider Addons For Elementor (Revolution of a slider, Hero Slider, Ecommerce Slider)	The Prime Slider - Addons For Elementor (Revolution of a slider, Hero Slider, Ecommerce Slider) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' attribute within the Pacific widget in all versions up to, and including, 3.14.7 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.	2024-06-07	6.4	CVE-2024-5640
Benoit Mercusot--Simple Popup Manager	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Benoit Mercusot Simple Popup Manager allows Stored XSS.This issue affects Simple Popup Manager: from n/a through 1.3.5.	2024-06-03	5.9	CVE-2024-34797
BetterAddons--Better Elementor Addons	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in BetterAddons Better Elementor Addons allows PHP Local File Inclusion.This issue affects Better Elementor Addons: from n/a through 1.4.1.	2024-06-04	6.5	CVE-2024-33541
BeyondTrust--BeyondInsight	Prior to 23.2, it is possible to perform arbitrary Server-Side requests via HTTP-based connectors within BeyondInsight, resulting in a server-side request forgery vulnerability.	2024-06-04	4.8	CVE-2024-4219
BeyondTrust--BeyondInsight	Prior to 23.1, an information disclosure vulnerability exists within BeyondInsight which can allow an attacker to enumerate usernames.	2024-06-04	4.3	CVE-2024-4220
biplob018--Image Hover Effects for Elementor with Lightbox and Flipbox	The Image Hover Effects for Elementor with Lightbox and Flipbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '_id', 'oxi_addons_f_title_tag', and 'content_description_tag' parameters in all versions up to, and including, 3.0.2 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.	2024-06-06	6.4	CVE-2024-5001
Born05--CraftCMS Plugin - Two-Factor Authentication	The CraftCMS plugin Two-Factor Authentication through 3.3.3 allows reuse of TOTP tokens multiple times within the validity period.	2024-06-06	4.8	CVE-2024-5658
Brainstorm Force--Spectra	Improper Restriction of Excessive Authentication Attempts vulnerability in Brainstorm Force Spectra allows Functionality Bypass.This issue affects Spectra: from n/a through 2.3.0.	2024-06-03	5.3	CVE-2023-23730
Brainstorm Force--Spectra	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Brainstorm Force Spectra allows Code Injection.This issue affects Spectra: from n/a through 2.3.0.	2024-06-03	5.3	CVE-2023-23735
Brainstorm Force--Spectra	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in Brainstorm Force Spectra allows Content Spoofing, Phishing.This issue affects Spectra: from n/a through 2.3.0.	2024-06-03	5.3	CVE-2023-23738
brainstormforce--Cards for Beaver Builder	The Cards for Beaver Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Cards widget in all versions up to, and including, 1.1.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-	2024-06-08	6.4	CVE-2024-5663

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
brainstormforce--SureTriggers Connect All Your Plugins, Apps, Tools & Automate Everything!	The SureTriggers - Connect All Your Plugins, Apps, Tools & Automate Everything! plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Trigger Link shortcode in all versions up to, and including, 1.0.47 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.	2024-06-04	6.4	CVE-2024-5485
brizy -- brizy-page_builder	The Brizy - Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the form name values in all versions up to, and including, 2.4.43 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.	2024-06-05	6.1	CVE-2024-2087
brizy -- brizy-page_builder	The Brizy - Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Custom Attributes for blocks in all versions up to, and including, 2.4.43 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.	2024-06-05	5.4	CVE-2024-1161
brizy -- brizy-page_builder	The Brizy - Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via post content in all versions up to, and including, 2.4.41 due to insufficient input sanitization performed only on the client side and insufficient output escaping. This makes it possible for authenticated attackers, with contributor access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-05	5.4	CVE-2024-1940
brizy -- brizy-page_builder	The Brizy - Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Link To' field of multiple widgets in all versions up to, and including, 2.4.43 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.	2024-06-05	5.4	CVE-2024-3667
Bryan Hadaway--Site Favicon	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Bryan Hadaway Site Favicon allows Stored XSS.This issue affects Site Favicon: from n/a through 0.2.	2024-06-03	5.9	CVE-2024-35642
Canonical Ltd.--Netplan	netplan leaks the private key of wireguard to local users. A security fix will be released soon.	2024-06-07	6.5	CVE-2022-4968
cartpauj--Cartpauj Register Captcha	: Improper Control of Interaction Frequency vulnerability in cartpauj Cartpauj Register Captcha allows Functionality Misuse.This issue affects Cartpauj Register Captcha: from n/a through 1.0.02.	2024-06-04	6.5	CVE-2023-40673
CeiKay--Tooltip CK	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CeiKay Tooltip CK tooltip-ck allows Stored XSS.This issue affects Tooltip CK: from n/a through 2.2.15.	2024-06-08	5.9	CVE-2024-35756
Ciprian Popescu--Block for Font Awesome	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Ciprian Popescu Block for Font Awesome allows Stored XSS.This issue affects Block for Font Awesome: from n/a through 1.4.4.	2024-06-08	6.5	CVE-2024-35705
Cisco--Cisco Unified Contact	A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct a stored XSS attack by exploiting an RFI vulnerability. This vulnerability is due to insufficient validation of	2024-06-05	4.8	CVE-2024-20405

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Center Enterprise	user-supplied input for specific HTTP requests that are sent to an affected device. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive information on the affected device.			
claudiosanches--Claudio Sanches Checkout Cielo for WooCommerce	The Claudio Sanches - Checkout Cielo for WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to insufficient payment validation in the update_order_status() function in all versions up to, and including, 1.1.0. This makes it possible for unauthenticated attackers to update the status of orders to paid bypassing payment.	2024-06-04	5.3	CVE-2024-1718
Codection--Import and export users and customers	Missing Authorization vulnerability in Codection Import and export users and customers.This issue affects Import and export users and customers: from n/a through 1.24.6.	2024-06-08	5.3	CVE-2024-22151
codeless -- cowidgets_-_elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Codeless Cowidgets - Elementor Addons allows Stored XSS.This issue affects Cowidgets - Elementor Addons: from n/a through 1.1.1.	2024-06-04	5.4	CVE-2024-35782
codelessthemes--Cowidgets Elementor Addons	The Cowidgets - Elementor Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'heading_tag' parameter in all versions up to, and including, 1.1.1 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.	2024-06-04	6.4	CVE-2024-4697
codename065--Download Manager	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wpdm_modal_login_form' shortcode in all versions up to, and including, 3.2.93 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.	2024-06-05	6.4	CVE-2024-4001
CodePeople, paypaldev--CP Contact Form with Paypal	Missing Authorization vulnerability in CodePeople, paypaldev CP Contact Form with Paypal allows Functionality Misuse.This issue affects CP Contact Form with Paypal: from n/a through 1.3.34.	2024-06-03	4.3	CVE-2023-27460
CodePeople--Calculated Fields Form	Missing Authorization vulnerability in CodePeople Calculated Fields Form allows Functionality Misuse.This issue affects Calculated Fields Form: from n/a through 1.1.120.	2024-06-03	4.3	CVE-2023-26523
CodePeople--Contact Form Email	Improper Restriction of Excessive Authentication Attempts vulnerability in CodePeople Contact Form Email allows Functionality Bypass.This issue affects Contact Form Email: from n/a through 1.3.41.	2024-06-04	5.3	CVE-2023-48318
CodePeople--Contact Form Email	Missing Authorization vulnerability in CodePeople Contact Form Email allows Functionality Misuse.This issue affects Contact Form Email: from n/a through 1.3.31.	2024-06-04	4.3	CVE-2023-28494
CodePeople--CP Multi View Event Calendar	Missing Authorization vulnerability in CodePeople CP Multi View Event Calendar allows Functionality Misuse.This issue affects CP Multi View Event Calendar: from n/a through 1.4.10.	2024-06-03	4.3	CVE-2023-28492

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
CodePeople--Search in Place	Missing Authorization vulnerability in CodePeople Search in Place allows Functionality Misuse.This issue affects Search in Place: from n/a through 1.0.104.	2024-06-03	4.3	CVE-2023-26521
Creative Motion, Will Bontrager Software, LLC--Woody ad snippets	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Creative Motion, Will Bontrager Software, LLC Woody ad snippets allows Stored XSS.This issue affects Woody ad snippets: from n/a through 2.4.10.	2024-06-08	5.9	CVE-2024-35751
CreativeThemes--Blocksy Companion	Server-Side Request Forgery (SSRF) vulnerability in CreativeThemes Blocksy Companion.This issue affects Blocksy Companion: from n/a through 2.0.42.	2024-06-03	4.4	CVE-2024-35633
creativethemeshq--Blocksy	The Blocksy theme for WordPress is vulnerable to Reflected Cross-Site Scripting via the custom_url parameter in all versions up to, and including, 2.0.50 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.	2024-06-05	6.4	CVE-2024-5439
CRM Perks.--Integration for Contact Form 7 and Constant Contact	Cross-Site Request Forgery (CSRF) vulnerability in CRM Perks. Integration for Contact Form 7 and Constant Contact.This issue affects Integration for Contact Form 7 and Constant Contact: from n/a through 1.1.5.	2024-06-03	4.3	CVE-2024-35632
cyberchimps--Responsive Addons Starter Templates, Advanced Features and Customizer Settings for Responsive Theme.	The Responsive Addons - Starter Templates, Advanced Features and Customizer Settings for Responsive Theme. plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's file uploader in all versions up to, and including, 3.0.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-05	6.4	CVE-2024-5222
CyberChimps--Responsive	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CyberChimps Responsive allows Stored XSS.This issue affects Responsive: from n/a through 5.0.3.	2024-06-04	6.5	CVE-2024-35654
cyclonetheme--Elegant Blocks	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in cyclonetheme Elegant Blocks allows Stored XSS.This issue affects Elegant Blocks: from n/a through 1.7.	2024-06-03	6.5	CVE-2024-34769
dain--snappy	iq80 Snappy is a compression/decompression library. When uncompressing certain data, Snappy tries to read outside the bounds of the given byte arrays. Because Snappy uses the JDK class `sun.misc.Unsafe` to speed up memory access, no additional bounds checks are performed and this has similar security consequences as out-of-bounds access in C or C++, namely it can lead to non-deterministic behavior or crash the JVM. iq80 Snappy is not actively maintained anymore. As quick fix users can upgrade to version 0.5.	2024-06-03	5.3	CVE-2024-36124
Devnath verma--WP Captcha	Improper Restriction of Excessive Authentication Attempts vulnerability in Devnath verma WP Captcha allows Functionality Bypass.This issue affects WP Captcha: from n/a through 2.0.0.	2024-06-04	5.3	CVE-2023-44235

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dextorlobo--Custom Dash	The Custom Dash plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.0.2 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.	2024-06-06	4.4	CVE-2024-4942
dfactory--Download Attachments	The Download Attachments plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'download-attachments' shortcode in all versions up to, and including, 1.3 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.	2024-06-04	6.4	CVE-2024-3230
Dulldusk--PHP File Manager	Vulnerability in Dulldusk's PHP File Manager affecting version 1.7.8. This vulnerability consists of an XSS through the fm_current_dir parameter of index.php. An attacker could send a specially crafted JavaScript payload to an authenticated user and partially hijack their browser session.	2024-06-06	6.1	CVE-2024-5673 cve-
duongancol--Boostify Header Footer Builder for Elementor	The Boostify Header Footer Builder for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'size' parameter in all versions up to, and including, 1.3.2 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.	2024-06-05	6.4	CVE-2024-5006
duongancol--Boostify Header Footer Builder for Elementor	The Boostify Header Footer Builder for Elementor plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the create_bhf_post function in all versions up to, and including, 1.3.3. This makes it possible for authenticated attackers, with subscriber-level access and above, to create pages or posts with arbitrary content.	2024-06-06	4.3	CVE-2024-4788
El tiempo--Weather Widget Pro	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in El tiempo Weather Widget Pro allows Stored XSS.This issue affects Weather Widget Pro: from n/a through 1.1.40.	2024-06-08	6.5	CVE-2024-35755
elearningfreak --insert_or_embed_articulate_content	The Insert or Embed Articulate Content into WordPress plugin through 4.3000000023 lacks validation of URLs when adding iframes, allowing attackers to inject an iFrame in the page and thus load arbitrary content from any page.	2024-06-04	5.4	CVE-2024-0756
EmailGPT--EmailGPT	The EmailGPT service contains a prompt injection vulnerability. The service uses an API service that allows a malicious user to inject a direct prompt and take over the service logic. Attackers can exploit the issue by forcing the AI service to leak the standard hard-coded system prompts and/or execute unwanted prompts. When engaging with EmailGPT by submitting a malicious prompt that requests harmful information, the system will respond by providing the requested data. This vulnerability can be exploited by any individual with access to the service.	2024-06-05	6.5	CVE-2024-5184
Enea Overclokk--Stellissimo Text Box	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Enea Overclokk Stellissimo Text Box allows Stored XSS.This issue affects Stellissimo Text Box: from n/a through 1.1.4.	2024-06-08	5.9	CVE-2024-35752
envothemes--Envo Extra	The Envo Extra plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'button_css_id' parameter within the Button widget in all versions up to, and including, 1.8.23 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and	2024-06-07	6.4	CVE-2024-5645

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
envoyproxy--envoy	Envoy is a cloud-native, open source edge and service proxy. A theoretical request smuggling vulnerability exists through Envoy if a server can be tricked into adding an upgrade header into a response. Per RFC https://www.rfc-editor.org/rfc/rfc7230#section-6.7 a server sends 101 when switching protocols. Envoy incorrectly accepts a 200 response from a server when requesting a protocol upgrade, but 200 does not indicate protocol switch. This opens up the possibility of request smuggling through Envoy if the server can be tricked into adding the upgrade header to the response.	2024-06-04	5.9	CVE-2024-23326
envoyproxy--envoy	Envoy is a cloud-native, open source edge and service proxy. A crash was observed in `EnvoyQuicServerStream::OnInitialHeadersComplete()` with following call stack. It is a use-after-free caused by QUICHE continuing push request headers after `StopReading()` being called on the stream. As after `StopReading()`, the HCM's `ActiveStream` might have already be destroyed and any up calls from QUICHE could potentially cause use after free.	2024-06-04	5.9	CVE-2024-32974
envoyproxy--envoy	Envoy is a cloud-native, open source edge and service proxy. There is a crash at `QuicheDataReader::PeekVarInt62Length()`. It is caused by integer underflow in the `QuicStreamSequencerBuffer::PeekRegion()` implementation.	2024-06-04	5.9	CVE-2024-32975
envoyproxy--envoy	Envoy is a cloud-native, open source edge and service proxy. There is a use-after-free in `HttpConnectionManager` (HCM) with `EnvoyQuicServerStream` that can crash Envoy. An attacker can exploit this vulnerability by sending a request without `FIN`, then a `RESET_STREAM` frame, and then after receiving the response, closing the connection.	2024-06-04	5.9	CVE-2024-34362
envoyproxy--envoy	Envoy is a cloud-native, open source edge and service proxy. Envoy exposed an out-of-memory (OOM) vector from the mirror response, since async HTTP client will buffer the response with an unbounded buffer.	2024-06-04	5.7	CVE-2024-34364
Essential Addons--Essential Addons for Elementor Pro	The Essential Addons for Elementor Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'eael_lightbox_open_btn_icon' parameter within the Lightbox & Modal widget in all versions up to, and including, 5.8.15 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.	2024-06-07	6.4	CVE-2024-5612
evmos--evmos	Evmos is the Ethereum Virtual Machine (EVM) Hub on the Cosmos Network. Users are able to delegate tokens that have not yet been vested. This affects employees and grantees who have funds managed via `ClawbackVestingAccount`. This affects 18.1.0 and earlier.	2024-06-06	5.3	CVE-2024-37154
extendthemes--Colibri Page Builder	The Colibri Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's colibri_video_player shortcode in all versions up to, and including, 1.0.276 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.	2024-06-07	6.4	CVE-2024-4451
extendthemes--Colibri Page Builder	The Colibri 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, 1.0.276 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.	2024-06-06	6.4	CVE-2024-5038

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Fahad Mahmood--WP Docs	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Fahad Mahmood WP Docs allows Stored XSS.This issue affects WP Docs: from n/a through 2.1.3.	2024-06-08	6.5	CVE-2024-35695
Fastly--Fastly	Missing Authorization vulnerability in Fastly.This issue affects Fastly: from n/a through 1.2.25.	2024-06-03	4.3	CVE-2024-34803
FeedbackWP--Rate my Post WP Rating System	Authentication Bypass by Spoofing vulnerability in FeedbackWP Rate my Post - WP Rating System allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Rate my Post - WP Rating System: from n/a through 3.4.2.	2024-06-04	5.3	CVE-2023-51667
flowdee--EasyAzon Amazon Associates Affiliate Plugin	The EasyAzon - Amazon Associates Affiliate Plugin plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'easyazon-cloaking-locale' parameter in all versions up to, and including, 5.1.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-06-06	6.1	CVE-2023-6956
Forge12 Interactive GmbH--Captcha/Honeypot for Contact Form 7	Improper Restriction of Excessive Authentication Attempts vulnerability in Forge12 Interactive GmbH Captcha/Honeypot for Contact Form 7 allows Functionality Bypass.This issue affects Captcha/Honeypot for Contact Form 7: from n/a through 1.11.3.	2024-06-04	5.3	CVE-2023-45009
Fortinet--FortiAuthenticator	A URL redirection to untrusted site ('open redirect') in Fortinet FortiAuthenticator version 6.6.0, version 6.5.3 and below, version 6.4.9 and below may allow an attacker to to redirect users to an arbitrary website via a crafted URL.	2024-06-03	6.1	CVE-2024-23664
Fortinet--FortiPortal	A client-side enforcement of server-side security in Fortinet FortiPortal version 6.0.0 through 6.0.14 allows attacker to improper access control via crafted HTTP requests.	2024-06-03	4.3	CVE-2023-48789
Fortinet--FortiSOAR	An improper removal of sensitive information before storage or transfer vulnerability [CWE-212] in FortiSOAR version 7.3.0, version 7.2.2 and below, version 7.0.3 and below may allow an authenticated low privileged user to read Connector passwords in plain-text via HTTP responses.	2024-06-03	6.5	CVE-2024-31493
Fortinet--FortiWeb	An exposure of sensitive information to an unauthorized actor vulnerability [CWE-200] in FortiWeb version 7.4.0, version 7.2.4 and below, version 7.0.8 and below, 6.3 all versions may allow an authenticated attacker to read password hashes of other administrators via CLI commands.	2024-06-03	5.5	CVE-2024-23107
Fortinet--FortiWeb	Multiple improper authorization vulnerabilities [CWE-285] in FortiWeb version 7.4.2 and below, version 7.2.7 and below, version 7.0.10 and below, version 6.4.3 and below, version 6.3.23 and below may allow an authenticated attacker to perform unauthorized ADOM operations via crafted requests.	2024-06-03	5.9	CVE-2024-23665
Fortinet--FortiWebManager	An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and 6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI.	2024-06-05	6.5	CVE-2024-23669
freephp-1--Nafeza Prayer Time	The Nafeza Prayer Time plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.2.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2024-06-04	4.4	CVE-2024-4462

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
g5theme--Essential Real Estate	The Essential Real Estate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ere_property_map' shortcode in all versions up to, and including, 4.4.2 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.	2024-06-04	6.4	CVE-2024-4273
g5theme--Essential Real Estate	The Essential Real Estate plugin for WordPress is vulnerable to unauthorized loss of data due to insufficient validation on the remove_property_attachment_ajax() function in all versions up to, and including, 4.4.2. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary attachments.	2024-06-04	4.3	CVE-2024-4274
GeneratePress--GP Premium	The GP Premium plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the message parameter in all versions up to, and including, 2.4.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-06-05	6.1	CVE-2024-3469
getbrave -- brave	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Brave Brave Popup Builder allows Stored XSS.This issue affects Brave Popup Builder: from n/a through 0.6.8.	2024-06-04	4.8	CVE-2024-35655
getformwork--formwork	Formwork is a flat file-based Content Management System (CMS). An attackers (requires administrator privilege) to execute arbitrary web scripts by modifying site options via /panel/options/site. This type of attack is suitable for persistence, affecting visitors across all pages (except the dashboard). This vulnerability is fixed in 1.13.1.	2024-06-07	4.8	CVE-2024-37160
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_lightbox shortcode in all versions up to, and including, 7.1.6 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.	2024-06-05	6.4	CVE-2024-4821
GregRoss--Just Writing Statistics	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in GregRoss Just Writing Statistics allows Stored XSS.This issue affects Just Writing Statistics: from n/a through 4.5.	2024-06-03	5.9	CVE-2024-35641
gVectors Team--wpDiscuz	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in gVectors Team wpDiscuz allows Stored XSS.This issue affects wpDiscuz: from n/a through 7.6.18.	2024-06-08	6.5	CVE-2024-35681
gVectors Team--wpDiscuz	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in gVectors Team wpDiscuz allows Code Injection.This issue affects wpDiscuz: from n/a through 7.6.10.	2024-06-04	5.3	CVE-2023-46310
Hans van Eijsden,niwreg--ImageMagick Sharpen Resized Images	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Hans van Eijsden,niwreg ImageMagick Sharpen Resized Images allows Stored XSS.This issue affects ImageMagick Sharpen Resized Images: from n/a through 1.1.7.	2024-06-03	5.9	CVE-2024-34790
HasThemes--HT Feed	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in HasThemes HT Feed allows Stored XSS.This issue affects HT Feed: from n/a through 1.2.8.	2024-06-08	6.5	CVE-2024-35699

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
HasThemes--ShopLentor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in HasThemes ShopLentor allows Stored XSS.This issue affects ShopLentor: from n/a through 2.8.7.	2024-06-03	6.5	CVE-2024-34767
HCL Software--Connections Docs	HCL Connections Docs is vulnerable to a cross-site scripting attack where an attacker may leverage this issue to execute arbitrary code. This may lead to credentials disclosure and possibly launch additional attacks.	2024-06-08	4.4	CVE-2023-45707
horearadu--Materialis Companion	The Materialis Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's materialis_contact_form shortcode in all versions up to, and including, 1.3.41 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.	2024-06-06	6.4	CVE-2024-4707
horearadu--One Page Express Companion	The One Page Express Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's one_page_express_contact_form shortcode in all versions up to, and including, 1.6.37 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.	2024-06-07	6.4	CVE-2024-4703
ibabar--WordPress prettyPhoto	The WordPress prettyPhoto plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter in all versions up to, and including, 1.2.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-06	6.4	CVE-2024-5162
IBM--i	IBM i 7.2, 7.3, 7.4, and 7.5 Service Tools Server (SST) is vulnerable to SST user enumeration by a remote attacker. This vulnerability can be used by a malicious actor to gather information about SST users that can be targeted in further attacks. IBM X-Force ID: 287538.	2024-06-07	5.3	CVE-2024-31878
IBM--System Storage DS8900F	IBM System Storage DS8900F 89.22.19.0, 89.30.68.0, 89.32.40.0, 89.33.48.0, 89.40.83.0, and 89.40.93.0 could allow a remote user to create an LDAP connection with a valid username and empty password to establish an anonymous connection. IBM X-Force ID: 279518.	2024-06-06	5	CVE-2024-22326
Icegram--Icegram	Missing Authorization vulnerability in Icegram.This issue affects Icegram: from n/a through 3.1.21.	2024-06-08	4.3	CVE-2024-21748
IdoPesok--zsa	zsa is a library for building typesafe server actions in Next.js. All users are impacted. The zsa application transfers the parse error stack from the server to the client in production build mode. This can potentially reveal sensitive information about the server environment, such as the machine username and directory paths. An attacker could exploit this vulnerability to gain unauthorized access to sensitive server information. This information could be used to plan further attacks or gain a deeper understanding of the server infrastructure. This has been patched on `0.3.3`.	2024-06-07	4	CVE-2024-37162
ILLID--Advanced Woo Labels	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ILLID Advanced Woo Labels allows Cross-Site Scripting (XSS).This issue affects Advanced Woo Labels: from n/a through 1.93.	2024-06-08	6.5	CVE-2024-35675
IP2Location--Download IP2Location Country Blocker	Authentication Bypass by Spoofing vulnerability in IP2Location Download IP2Location Country Blocker allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Download IP2Location Country Blocker: from n/a through 2.29.1.	2024-06-04	5.3	CVE-2023-37865

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ishanverma--Authorize.net Payment Gateway For WooCommerce	The Authorize.net Payment Gateway For WooCommerce plugin for WordPress is vulnerable to payment bypass in all versions up to, and including, 8.0. This is due to the plugin not properly verifying the authenticity of the request that updates a orders payment status. This makes it possible for unauthenticated attackers to update order payment statuses to paid bypassing any payment.	2024-06-04	5.3	CVE-2024-2382
itsourcecode--Bakery Online Ordering System	A vulnerability was found in itsourcecode Bakery Online Ordering System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file index.php. The manipulation of the argument txtsearch 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-267091.	2024-06-04	6.3	CVE-2024-5635
itsourcecode--Bakery Online Ordering System	A vulnerability was found in itsourcecode Bakery Online Ordering System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file report/index.php. The manipulation of the argument procduct 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-267092.	2024-06-05	6.3	CVE-2024-5636
itsourcecode--Online Discussion Forum	A vulnerability classified as critical has been found in itsourcecode Online Discussion Forum 1.0. Affected is an unknown function of the file /members/poster.php. The manipulation of the argument image leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-267408.	2024-06-07	6.3	CVE-2024-5734
J.N. Breetvelt a.k.a. OpaJaap--WP Photo Album Plus	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in J.N. Breetvelt a.K.A. OpaJaap WP Photo Album Plus allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects WP Photo Album Plus: from n/a through 8.5.02.005.	2024-06-04	5.3	CVE-2023-49774
j0hnsmith--Testimonials Widget	The Testimonials Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's testimonials shortcode in all versions up to, and including, 4.0.4 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.	2024-06-06	6.4	CVE-2024-4705
Jewel Theme--Master Addons for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jewel Theme Master Addons for Elementor allows Stored XSS.This issue affects Master Addons for Elementor: from n/a through 2.0.5.9.	2024-06-08	6.5	CVE-2024-35688
Jewel Theme--Master Addons for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jewel Theme Master Addons for Elementor allows Stored XSS.This issue affects Master Addons for Elementor: from n/a through 2.0.6.0.	2024-06-08	6.5	CVE-2024-35702
johnnash1975--Easy Social Like Box Popup Sidebar Widget	The Easy Social Like Box - Popup - Sidebar Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'cardoza_facebook_like_box' shortcode in all versions up to, and including, 4.0 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.	2024-06-06	6.4	CVE-2024-5224
JumpDEMAND Inc.--ActiveDEMAND	Cross-Site Request Forgery (CSRF) vulnerability in JumpDEMAND Inc. ActiveDEMAND.This issue affects ActiveDEMAND: from n/a through 0.2.43.	2024-06-03	4.3	CVE-2024-35638

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Kharim Tomlinson--WP Next Post Navi	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kharim Tomlinson WP Next Post Navi allows Stored XSS.This issue affects WP Next Post Navi: from n/a through 1.8.3.	2024-06-03	5.9	CVE-2024-34793
Kognetiks--Kognetiks Chatbot for WordPress	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kognetiks Kognetiks Chatbot for WordPress allows Stored XSS.This issue affects Kognetiks Chatbot for WordPress: from n/a through 1.9.8.	2024-06-08	6.5	CVE-2024-35738
LabVantage--LIMS	A vulnerability classified as critical was found in LabVantage LIMS 2017. This vulnerability affects unknown code of the file /labvantage/rc?command=page&page=SampleList&_iframename=list of the component POST Request Handler. The manipulation of the argument param1 leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-267454 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-08	6.3	CVE-2024-5771
Lester GaMerZ Chan--WP-PostRatings	Improper Control of Interaction Frequency vulnerability in Lester 'GaMerZ' Chan WP-PostRatings allows Functionality Misuse.This issue affects WP-PostRatings: from n/a through 1.91.	2024-06-04	5.3	CVE-2023-40332
litonice13--Master Addons Free Widgets, Hover Effects, Toggle, Conditions, Animations for Elementor	The Master Addons - Free Widgets, Hover Effects, Toggle, Conditions, Animations for Elementor plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ma-template' REST API route in all versions up to, and including, 2.0.6.1. This makes it possible for unauthenticated attackers to create or modify existing Master Addons templates or make settings modifications related to these templates.	2024-06-07	6.5	CVE-2024-5382
Lukman Nakib--Debug Log Manger Tool	Insertion of Sensitive Information into Log File vulnerability in Lukman Nakib Debug Log - Manger Tool.This issue affects Debug Log - Manger Tool: from n/a through 1.4.5.	2024-06-03	5.3	CVE-2024-34798
MagniGenie--RestroPress	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in MagniGenie RestroPress allows Stored XSS.This issue affects RestroPress: from n/a through 3.1.2.1.	2024-06-08	6.5	CVE-2024-35719
Marketing Fire, LLC--Widget Options - Extended	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Marketing Fire, LLC Widget Options - Extended.This issue affects Widget Options - Extended: from n/a through 5.1.0.	2024-06-08	6.5	CVE-2024-35691
melapress--Admin Notices Manager	The Admin Notices Manager plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the handle_ajax_call() function in all versions up to, and including, 1.4.0. This makes it possible for authenticated attackers, with subscriber-level access and above, to retrieve a list of registered user emails.	2024-06-04	4.3	CVE-2024-1717
Menno Luitjes--Foyer	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Menno Luitjes Foyer allows Code Injection.This issue affects Foyer: from n/a through 1.7.5.	2024-06-04	4.6	CVE-2023-47663
Mervin Praison--Praison SEO WordPress	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Mervin Praison Praison SEO WordPress allows Stored XSS.This issue affects Praison SEO WordPress: from n/a through 4.0.15.	2024-06-03	6.5	CVE-2024-34801

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
metagauss--ProfileGrid User Profiles, Groups and Communities	The ProfileGrid - User Profiles, Groups and Communities plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the pm_dismissible_notice and pm_wizard_update_group_icon functions in all versions up to, and including, 5.8.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change arbitrary options to the value '1' or change group icons.	2024-06-05	4.3	CVE-2024-5453
Metagauss--RegistrationMagic	Authentication Bypass by Spoofing vulnerability in Metagauss RegistrationMagic allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects RegistrationMagic: from n/a through 5.2.5.0.	2024-06-04	5.3	CVE-2023-51543
Metagauss--RegistrationMagic	Improper Control of Interaction Frequency vulnerability in Metagauss RegistrationMagic allows Functionality Misuse.This issue affects RegistrationMagic: from n/a through 5.2.5.0.	2024-06-04	5.3	CVE-2023-51544
miniorange--Malware Scanner	Authentication Bypass by Spoofing vulnerability in miniorange Malware Scanner allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Malware Scanner: from n/a through 4.7.1.	2024-06-04	5.3	CVE-2023-52176
MongoDB Inc--PyMongo	An out-of-bounds read in the 'bson' module of PyMongo 4.6.2 or earlier allows deserialization of malformed BSON provided by a Server to raise an exception which may contain arbitrary application memory.	2024-06-05	4.7	CVE-2024-5629 cna@mongodb.com
moveaddons--Move Addons for Elementor	Missing Authorization vulnerability in moveaddons Move Addons for Elementor.This issue affects Move Addons for Elementor: from n/a through 1.2.9.	2024-06-04	5.3	CVE-2024-30525
mpntod--Rotating Tweets (Twitter widget and shortcode)	The Rotating Tweets (Twitter widget and shortcode) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's' 'rotatingtweets' in all versions up to, and including, 1.9.10 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.	2024-06-06	6.4	CVE-2024-5141
N/A--Church Admin	Server-Side Request Forgery (SSRF) vulnerability in Church Admin.This issue affects Church Admin: from n/a through 4.3.6.	2024-06-03	4.4	CVE-2024-35637
N/A--KiviCare	Authorization Bypass Through User-Controlled Key vulnerability in KiviCare.This issue affects KiviCare: from n/a through 3.6.2.	2024-06-08	5.3	CVE-2024-35659
n/a--n/a	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_nan_config_get_nl_params(), there is no input validation check on hal_req->num_config_discovery_attr coming from userspace, which can lead to a heap overwrite.	2024-06-05	6.7	CVE-2024-27370
n/a--n/a	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_nan_followup_get_nl_params(), there is no input validation check on hal_req->service_specific_info_len coming from userspace, which can lead to a heap overwrite.	2024-06-05	6.7	CVE-2024-27371
n/a--n/a	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_nan_config_get_nl_params(), there is no input validation check on disc_attr->infrastructure_ssid_len coming from userspace, which can lead to a heap overwrite.	2024-06-05	6.7	CVE-2024-27372

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_nan_config_get_nl_params(), there is no input validation check on disc_attr->mesh_id_len coming from userspace, which can lead to a heap overwrite.	2024-06-05	6.7	CVE-2024-27373
n/a--n/a	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_nan_publish_get_nl_params(), there is no input validation check on hal_req->service_specific_info_len coming from userspace, which can lead to a heap overwrite.	2024-06-05	6.7	CVE-2024-27374
n/a--n/a	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_nan_followup_get_nl_params(), there is no input validation check on hal_req->sdea_service_specific_info_len coming from userspace, which can lead to a heap overwrite.	2024-06-05	6.7	CVE-2024-27375
n/a--n/a	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_nan_subscribe_get_nl_params(), there is no input validation check on hal_req->rx_match_filter_len coming from userspace, which can lead to a heap overwrite.	2024-06-05	6.7	CVE-2024-27376
n/a--n/a	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_nan_get_security_info_nl(), there is no input validation check on sec_info->key_info.body.pmk_info.pmk_len coming from userspace, which can lead to a heap overwrite.	2024-06-05	6.7	CVE-2024-27377
n/a--n/a	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_send_action_frame_cert(), there is no input validation check on len coming from userspace, which can lead to a heap over-read.	2024-06-05	6	CVE-2024-27378
n/a--n/a	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_nan_subscribe_get_nl_params(), there is no input validation check on hal_req->num_intf_addr_present coming from userspace, which can lead to a heap overwrite.	2024-06-05	6.7	CVE-2024-27379
n/a--n/a	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_set_delayed_wakeup_type(), there is no input validation check on a length of ioctl_args->args[i] coming from userspace, which can lead to a heap over-read.	2024-06-05	6	CVE-2024-27380
n/a--n/a	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_send_action_frame_ut(), there is no input validation check on len coming from userspace, which can lead to a heap over-read.	2024-06-05	6	CVE-2024-27381
n/a--n/a	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_send_action_frame(), there is no input validation check on len coming from userspace, which can lead to a heap over-read.	2024-06-05	6	CVE-2024-27382
n/a--n/a	An issue was discovered in Samsung Mobile Processor EExynos 2200, Exynos 1480, Exynos 2400. It lacks a check for the validation of native handles, which can result in an Out-of-Bounds Write.	2024-06-07	6.8	CVE-2024-31958
n/a--n/a	Ariane Allegro Scenario Player through 2024-03-05, when Ariane Duo kiosk mode is used, allows physically proximate attackers to obtain sensitive information (such as hotel invoice content with PII), and potentially create unauthorized room keys, by	2024-06-06	6.8	CVE-2024-37364

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	entering a guest-search quote character and then accessing the underlying Windows OS.			
n/a--n/a	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption.	2024-06-05	5.3	CVE-2023-49927
n/a--n/a	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) module. This can lead to disclosure of sensitive information.	2024-06-05	5.9	CVE-2024-28818
n/a--n/a	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information.	2024-06-04	5.9	CVE-2024-29152
N/A--RT Easy Builder Advanced addons for Elementor	Missing Authorization vulnerability in RT Easy Builder - Advanced addons for Elementor.This issue affects RT Easy Builder - Advanced addons for Elementor: from n/a through 2.0.	2024-06-04	4.3	CVE-2024-30484
nalam-1--Magical Addons For Elementor (Header Footer Builder, Free Elementor Widgets, Elementor Templates Library)	The Magical Addons For Elementor (Header Footer Builder, Free Elementor Widgets, Elementor Templates Library) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '_id' parameter in all versions up to, and including, 1.1.39 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.	2024-06-06	6.4	CVE-2024-5161
nayrathemes--Clever Fox	The Clever Fox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's info box block in all versions up to, and including, 25.2.0 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.	2024-06-07	6.4	CVE-2024-1768
nayrathemes--Clever Fox	The Clever Fox - One Click Website Importer by Nayra Themes plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'clever-fox-activate-theme' function in all versions up to, and including, 25.2.0. This makes it possible for authenticated attackers, with subscriber access and above, to modify the active theme, including to an invalid value which can take down the site.	2024-06-07	5.4	CVE-2023-6876
ndijkstra--Mollie Forms	The Mollie Forms plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.6.13. This is due to missing or incorrect nonce validation on the duplicateForm() function. This makes it possible for unauthenticated attackers to duplicate forms via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-06-05	4.3	CVE-2024-2368
Netentsec--NS-ASG Application	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3. It has been classified as critical. This affects an unknown part of the file	2024-06-03	6.3	CVE-2024-5589

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Security Gateway	/admin/config_MT.php?action=delete. The manipulation of the argument Mid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-266847. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
Netentsec--NS-ASG Application Security Gateway	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3. It has been declared as critical. This vulnerability affects unknown code of the file /protocol/iscuser/uploadiscuser.php of the component JSON Content Handler. The manipulation of the argument messagecontent 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-266848. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-03	6.3	CVE-2024-5590
netty--netty-incubator-codec-ohttp	netty-incubator-codec-ohttp is the OHTTP implementation for netty. BoringSSLAEADContext keeps track of how many OHTTP responses have been sent and uses this sequence number to calculate the appropriate nonce to use with the encryption algorithm. Unfortunately, two separate errors combine which would allow an attacker to cause the sequence number to overflow and thus the nonce to repeat.	2024-06-04	5.9	CVE-2024-36121
Nitin Rathod--WP Forms Puzzle Captcha	Improper Restriction of Excessive Authentication Attempts vulnerability in Nitin Rathod WP Forms Puzzle Captcha allows Functionality Bypass.This issue affects WP Forms Puzzle Captcha: from n/a through 4.1.	2024-06-04	5.3	CVE-2023-48276
oslabs-beta--SkyScraper	SkyScrape is a GUI Dashboard for AWS Infrastructure and Managing Resources and Usage Costs. SkyScrape's API requests are currently unsecured HTTP requests, leading to potential vulnerabilities for the user's temporary credentials and data. This affects version 1.0.0.	2024-06-07	6.4	CVE-2024-37163
OTRS AG--OTRS	The file upload feature in OTRS and ((OTRS)) Community Edition has a path traversal vulnerability. This issue permits authenticated agents or customer users to upload potentially harmful files to directories accessible by the web server, potentially leading to the execution of local code like Perl scripts. This issue affects OTRS: from 7.0.X through 7.0.49, 8.0.X, 2023.X, from 2024.X through 2024.3.2; ((OTRS)) Community Edition: from 6.0.1 through 6.0.34.	2024-06-06	6.3	CVE-2024-23793 security@otrs.com
pandaboxwp--WP jQuery Lightbox	The WP jQuery Lightbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title' attribute in all versions up to, and including, 1.5.4 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.	2024-06-07	6.4	CVE-2024-5425
pdfcrowd --save_as_pdf_plugin	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Pdfcrowd Save as PDF plugin by Pdfcrowd allows Stored XSS.This issue affects Save as PDF plugin by Pdfcrowd: from n/a through 3.2.3.	2024-06-04	5.4	CVE-2024-35649
Peregrine themes--Bloglo	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Peregrine themes Bloglo allows Stored XSS.This issue affects Bloglo: from n/a through 1.1.3.	2024-06-08	6.5	CVE-2024-35715
pickplugins--Gutenberg Blocks, Page Builder ComboBlocks	The Post Grid, Form Maker, Popup Maker, WooCommerce Blocks, Post Blocks, Post Carousel - Combo Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tag' attribute in blocks in all versions up to, and including, 2.2.80 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.	2024-06-07	6.4	CVE-2024-1988

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pickplugins--Gutenberg Blocks, Page Builder ComboBlocks	The Post Grid, Form Maker, Popup Maker, WooCommerce Blocks, Post Blocks, Post Carousel - Combo Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'class' attribute of the menu-wrap-item block in all versions up to, and including, 2.2.80 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.	2024-06-07	6.4	CVE-2024-4042
PickPlugins--Tabs & Accordion	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in PickPlugins Tabs & Accordion allows Code Injection.This issue affects Tabs & Accordion: from n/a through 1.3.10.	2024-06-04	5.4	CVE-2023-40557
PINPOINT.WORLD--Pinpoint Booking System	External Control of Assumed-Immutable Web Parameter vulnerability in PINPOINT.WORLD Pinpoint Booking System allows Functionality Misuse.This issue affects Pinpoint Booking System: from n/a through 2.9.9.3.4.	2024-06-04	6.5	CVE-2023-38520
Plechev Andrey--WP-Recall	Cross-Site Request Forgery (CSRF) vulnerability in Plechev Andrey WP-Recall.This issue affects WP-Recall: from n/a through 16.26.6.	2024-06-08	5.4	CVE-2024-35657
Pluggabl LLC--Booster Elite for WooCommerce	Improper Authentication vulnerability in Pluggabl LLC Booster Elite for WooCommerce allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Booster Elite for WooCommerce: from n/a before 7.1.3.	2024-06-04	6.5	CVE-2023-51511
Pluggabl LLC--Booster for WooCommerce	Improper Authentication vulnerability in Pluggabl LLC Booster for WooCommerce allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Booster for WooCommerce: from n/a through 7.1.2.	2024-06-04	6.5	CVE-2023-48747
pluginever--WP Content Pilot Autoblogging & Affiliate Marketing Plugin	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in pluginever WP Content Pilot - Autoblogging & Affiliate Marketing Plugin allows Code Injection.This issue affects WP Content Pilot - Autoblogging & Affiliate Marketing Plugin: from n/a through 1.3.3.	2024-06-04	4.3	CVE-2023-45053
pluginkollektiv--Antispam Bee	Authentication Bypass by Spoofing vulnerability in pluginkollektiv Antispam Bee allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Antispam Bee: from n/a through 2.11.3.	2024-06-04	5.3	CVE-2023-41134
Podlove--Podlove Web Player	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Podlove Podlove Web Player.This issue affects Podlove Web Player: from n/a through 5.7.3.	2024-06-08	5.3	CVE-2024-35710
Popup Maker--Popup Maker WP	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Popup Maker Popup Maker WP allows Stored XSS.This issue affects Popup Maker WP: from n/a through 1.2.8.	2024-06-03	6.5	CVE-2024-34770
POSIMYTH--The Plus Addons for Elementor Page Builder Lite	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in POSIMYTH The Plus Addons for Elementor Page Builder Lite allows Stored XSS.This issue affects The Plus Addons for Elementor Page Builder Lite: from n/a through 5.5.4.	2024-06-08	6.5	CVE-2024-35709
PropertyHive--PropertyHive	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PropertyHive allows Stored XSS.This issue affects PropertyHive: from n/a through 2.0.13.	2024-06-08	6.5	CVE-2024-35701
ptz0n--Google CSE	The Google CSE plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.0.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated	2024-06-06	4.4	CVE-2024-5656

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			
Pure Chat by Ruby--Pure Chat	Cross-Site Request Forgery (CSRF) vulnerability in Pure Chat by Ruby Pure Chat.This issue affects Pure Chat: from n/a through 2.22.	2024-06-05	4.3	CVE-2024-35673
purvabathe--Simple Image Popup Shortcode	The Simple Image Popup Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'sips_popup' shortcode in all versions up to, and including, 1.0 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.	2024-06-06	6.4	CVE-2024-5342
qodeinteractive--Qi Addons For Elementor	The Qi Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's button widgets in all versions up to, and including, 1.7.2 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.	2024-06-06	6.4	CVE-2024-4364
qodeinteractive--Qi Blocks	The Qi Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's file uploader in all versions up to, and including, 1.2.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-06	6.4	CVE-2024-5221
Qualcomm, Inc.--Snapdragon	Information disclosure while handling T2LM Action Frame in WLAN Host.	2024-06-03	6.5	CVE-2023-43537
Qualcomm, Inc.--Snapdragon	Memory corruption in Audio during a playback or a recording due to race condition between allocation and deallocation of graph object.	2024-06-03	6.7	CVE-2023-43543
Qualcomm, Inc.--Snapdragon	Memory corruption when IPC callback handle is used after it has been released during register callback by another thread.	2024-06-03	6.7	CVE-2023-43544
Qualcomm, Inc.--Snapdragon	Memory corruption when more scan frequency list or channels are sent from the user space.	2024-06-03	6.7	CVE-2023-43545
Qualcomm, Inc.--Snapdragon	transient DOS when setting up a fence callback to free a KGSL memory entry object during DMA.	2024-06-03	6.2	CVE-2024-21478
quomodosoft--ElementsReady Addons for Elementor	The ElementsReady Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '_id' parameter in all versions up to, and including, 6.1.0 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.	2024-06-06	6.4	CVE-2024-5152
RadiusTheme--The Post Grid	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in RadiusTheme The Post Grid allows Stored XSS.This issue affects The Post Grid: from n/a through 7.7.1.	2024-06-08	6.5	CVE-2024-35739
rails--rails	Action Text brings rich text content and editing to Rails. Instances of ActionText::Attachable::ContentAttachment included within a rich_text_area tag	2024-06-04	6.1	CVE-2024-32464

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	could potentially contain unsanitized HTML. This vulnerability is fixed in 7.1.3.4 and 7.2.0.beta2.			
rails--rails	Action Pack is a framework for handling and responding to web requests. Since 6.1.0, the application configurable Permissions-Policy is only served on responses with an HTML related Content-Type. This vulnerability is fixed in 6.1.7.8, 7.0.8.2, and 7.1.3.3.	2024-06-04	5.4	CVE-2024-28103
Red Hat--Red Hat Satellite 6	A flaw was found in foreman-installer when puppet-candlepin is invoked cpdb with the --password parameter. This issue leaks the password in the process list and allows an attacker to take advantage and obtain the password.	2024-06-05	6.2	CVE-2024-3716
Red Hat--Red Hat Satellite 6	A flaw was found in the Katello plugin for Foreman, where it is possible to store malicious JavaScript code in the "Description" field of a user. This code can be executed when opening certain pages, for example, Host Collections.	2024-06-05	4.8	CVE-2024-4812
restrict--Restrict for Elementor	The Restrict for Elementor plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.0.6 due to improper restrictions on hidden data that make it accessible through the REST API. This makes it possible for unauthenticated attackers to extract potentially sensitive data from post content.	2024-06-06	5.3	CVE-2024-0910
Revolution Slider--Slider Revolution	The Slider Revolution plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Add Layer widget in all versions up to, and including, 6.7.11 due to insufficient input sanitization and output escaping on the user supplied 'class', 'id', and 'title' attributes. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. NOTE: Successful exploitation of this vulnerability requires an Administrator to give Slider Creation privileges to Author-level users.	2024-06-04	6.4	CVE-2024-4581
Revolution Slider--Slider Revolution	The Slider Revolution plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 6.7.10 due to insufficient input sanitization and output escaping on the user supplied Elementor 'wrapperid' and 'zindex' display 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.	2024-06-04	6.4	CVE-2024-4637
rubengc--GamiPress Link	The GamiPress - Link plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's gamipress_link shortcode in all versions up to, and including, 1.1.4 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.	2024-06-05	6.4	CVE-2024-5536
rustaurius--Five Star Restaurant Menu and Food Ordering	The Restaurant Menu and Food Ordering plugin for WordPress is vulnerable to unauthorized creation of data due to a missing capability check on 'add_section', 'add_menu', 'add_menu_item', and 'add_menu_page' functions in all versions up to, and including, 2.4.16. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create menu sections, menus, food items, and new menu pages.	2024-06-05	4.3	CVE-2024-5459
Samsung Mobile--GalaxyBudsManager PC	Arbitrary directory creation in GalaxyBudsManager PC prior to version 2.1.240315.51 allows attacker to create arbitrary directory.	2024-06-04	6.2	CVE-2024-20887
Samsung Mobile--Samsung Live Wallpaper PC	Arbitrary directory creation in Samsung Live Wallpaper PC prior to version 3.3.8.0 allows attacker to create arbitrary directory.	2024-06-04	6.2	CVE-2024-20886

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Samsung Mobile--Samsung Mobile Devices	Improper input validation in libsheifdecadapter.so prior to SMR Jun-2024 Release 1 allows local attackers to lead to memory corruption.	2024-06-04	6.1	CVE-2024-20876
Samsung Mobile--Samsung Mobile Devices	Stack-based buffer overflow vulnerability in bootloader prior to SMR Jun-2024 Release 1 allows physical attackers to overwrite memory.	2024-06-04	6.4	CVE-2024-20880
Samsung Mobile--Samsung Mobile Devices	Improper input validation vulnerability in chnactiv TA prior to SMR Jun-2024 Release 1 allows local privileged attackers lead to potential arbitrary code execution.	2024-06-04	6.4	CVE-2024-20881
Samsung Mobile--Samsung Mobile Devices	Incorrect use of privileged API vulnerability in registerBatteryStatsCallback in BatteryStatsService prior to SMR Jun-2024 Release 1 allows local attackers to use privileged API.	2024-06-04	6.2	CVE-2024-20883
Samsung Mobile--Samsung Mobile Devices	Incorrect use of privileged API vulnerability in getSemBatteryUsageStats in BatteryStatsService prior to SMR Jun-2024 Release 1 allows local attackers to use privileged API.	2024-06-04	6.2	CVE-2024-20884
Samsung Mobile--Samsung Mobile Devices	Improper component protection vulnerability in Samsung Dialer prior to SMR May-2024 Release 1 allows local attackers to make a call without proper permission.	2024-06-04	5.1	CVE-2024-20885
Samsung Mobile--Samsung Mobile Devices	Improper input validation vulnerability in caminfo driver prior to SMR Jun-2024 Release 1 allows local privileged attackers to write out-of-bounds memory.	2024-06-04	4.2	CVE-2024-20873
Samsung Mobile--Samsung Mobile Devices	Improper caller verification vulnerability in SemClipboard prior to SMR June-2024 Release 1 allows local attackers to access arbitrary files.	2024-06-04	4	CVE-2024-20875
Samsung Mobile--Samsung Mobile Devices	Improper input validation vulnerability in libsavscmn.so prior to SMR Jun-2024 Release 1 allows local attackers to write out-of-bounds memory.	2024-06-04	4	CVE-2024-20879
Samsung Mobile--Samsung Mobile Devices	Out-of-bounds read vulnerability in bootloader prior to SMR June-2024 Release 1 allows physical attackers to arbitrary data access.	2024-06-04	4.6	CVE-2024-20882
satollo--Newsletter Send awesome emails from WordPress	The Newsletter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'np1' parameter in all versions up to, and including, 8.3.4 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.	2024-06-05	6.4	CVE-2024-5317
sendinblue -- newsletter\,_smtp\,_email_marketing_and_subscribe	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Brevo Newsletter, SMTP, Email marketing and Subscribe forms by Sendinblue allows Reflected XSS.This issue affects Newsletter, SMTP, Email marketing and Subscribe forms by Sendinblue: from n/a through 3.1.77.	2024-06-04	6.1	CVE-2024-35668

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Sensei--Sensei Pro (WC Paid Courses)	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Sensei Sensei Pro (WC Paid Courses) allows Stored XSS.This issue affects Sensei Pro (WC Paid Courses): from n/a through 4.23.1.1.23.1.	2024-06-08	6.5	CVE-2024-34765
shafayat-alam--Gutenberg Blocks and Page Layouts Attire Blocks	The Gutenberg Blocks and Page Layouts - Attire Blocks plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the disable_fe_assets function in all versions up to, and including, 1.9.2. This makes it possible for authenticated attackers, with subscriber access or above, to change the plugin's settings. Additionally, no nonce check is performed resulting in a CSRF vulnerability.	2024-06-05	4.3	CVE-2024-4088
shrinitech--Fluid Notification Bar	The Fluid Notification Bar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.2.3 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.	2024-06-04	4.4	CVE-2024-3031
silabs.com--Gecko SDK	A bug exists in the API, mesh_node_power_off(), which fails to copy the contents of the Replay Protection List (RPL) from RAM to NVM before powering down, resulting in the ability to replay unsaved messages. Note that as of June 2024, the Gecko SDK was renamed to the Simplicity SDK, and the versioning scheme was changed from Gecko SDK vX.Y.Z to Simplicity SDK YYYY.MM.Patch#.	2024-06-06	5.6	CVE-2024-4013
SinaExtra--Sina Extension for Elementor	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in SinaExtra Sina Extension for Elementor allows PHP Local File Inclusion.This issue affects Sina Extension for Elementor: from n/a through 3.5.1.	2024-06-04	6.5	CVE-2024-34384
SinaExtra--Sina Extension for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in SinaExtra Sina Extension for Elementor allows Stored XSS.This issue affects Sina Extension for Elementor: from n/a through 3.5.3.	2024-06-08	6.5	CVE-2024-35703
SoftLab--Integrate Google Drive	Broken Authentication vulnerability in SoftLab Integrate Google Drive.This issue affects Integrate Google Drive: from n/a through 1.3.93.	2024-06-04	5.3	CVE-2024-35670
solarwinds -- solarwinds_platform	The SolarWinds Platform was determined to be affected by a stored cross-site scripting vulnerability affecting the web console. A high-privileged user and user interaction is required to exploit this vulnerability.	2024-06-04	4.8	CVE-2024-29004
Spiffy Plugins--Spiffy Calendar	Missing Authorization vulnerability in Spiffy Plugins Spiffy Calendar.This issue affects Spiffy Calendar: from n/a through 4.9.10.	2024-06-04	5.4	CVE-2024-30528
spiffyplugins -- wp_flow_plus	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Spiffy Plugins WP Flow Plus allows Stored XSS.This issue affects WP Flow Plus: from n/a through 5.2.2.	2024-06-04	5.4	CVE-2024-35651
StarCitizenTools--mediawiki-skins-Citizen	Citizen is a MediaWiki skin that makes extensions part of the cohesive experience. The page `MediaWiki:Tagline` has its contents used unescaped, so custom HTML (including Javascript) can be injected by someone with the ability to edit the MediaWiki namespace (typically those with the `editinterface` permission, or sysops). This vulnerability is fixed in 2.16.0.	2024-06-03	6.5	CVE-2024-36123
sulu--SuluFormBundle	The SuluFormBundle adds support for creating dynamic forms in Sulu Admin. The TokenController get parameter formName is not sanitized in the returned input field which leads to XSS. This vulnerability is fixed in 2.5.3.	2024-06-06	6.1	CVE-2024-37156

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Synology--Camera Firmware	A vulnerability regarding buffer copy without checking the size of input ('Classic Buffer Overflow') has been found in the login component. This allows remote attackers to conduct denial-of-service attacks via unspecified vectors. This attack only affects the login service which will automatically restart. The following models with Synology Camera Firmware versions before 1.1.1-0383 may be affected: BC500 and TC500.	2024-06-04	6.5	CVE-2024-5463
tagDiv--tagDiv Composer	The tagDiv Composer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's button shortcode in all versions up to, and including, 4.8 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: The vulnerable code in this plugin is specifically tied to the tagDiv Newspaper theme. If another theme is installed (e.g., NewsMag), this code may not be present.	2024-06-04	6.4	CVE-2024-3888
Tainacan.org--Tainacan	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Tainacan.Org Tainacan allows Stored XSS.This issue affects Tainacan: from n/a through 0.21.3.	2024-06-03	6.5	CVE-2024-34795
takanakui--WP Mobile Menu The Mobile-Friendly Responsive Menu	The WP Mobile Menu - The Mobile-Friendly Responsive Menu plugin for WordPress is vulnerable to Stored Cross-Site Scripting via image alt text in all versions up to, and including, 2.8.4.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-07	5.4	CVE-2024-3987
Team Heateor--Heateor Social Login	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Team Heateor Heateor Social Login allows Stored XSS.This issue affects Heateor Social Login: from n/a through 1.1.32.	2024-06-08	6.5	CVE-2024-35707
TemplatesNext--TemplatesNext OnePager	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in TemplatesNext TemplatesNext OnePager allows Stored XSS.This issue affects TemplatesNext OnePager: from n/a through 1.3.3.	2024-06-08	6.5	CVE-2024-35753
Theme Freesia--Event	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Theme Freesia Event allows Stored XSS.This issue affects Event: from n/a through 1.2.2.	2024-06-08	6.5	CVE-2024-35711
Theme Freesia--Idyllic	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Theme Freesia Idyllic allows Stored XSS.This issue affects Idyllic: from n/a through 1.1.8.	2024-06-08	6.5	CVE-2024-35714
Theme Freesia--Pixgraphy	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Theme Freesia Pixgraphy allows Stored XSS.This issue affects Pixgraphy: from n/a through 1.3.8.	2024-06-08	6.5	CVE-2024-35740
themefarmer--WooCommerce Tools	The WooCommerce Tools plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the woocommerce_tool_toggle_module() function in all versions up to, and including, 1.2.9. This makes it possible for authenticated attackers, with subscriber-level access and above, to deactivate arbitrary plugin modules.	2024-06-07	5.3	CVE-2024-1689
themefusecom--Brizy Page Builder	The Brizy - Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's contact form widget error message and redirect URL in all versions up to, and including, 2.4.43 due to insufficient input sanitization and output escaping on user supplied error messages. This makes it possible for authenticated attackers with contributor-level and above permissions to inject	2024-06-05	6.4	CVE-2024-1164

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.			
Themeisle--Otter Blocks PRO	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Themeisle Otter Blocks PRO.This issue affects Otter Blocks PRO: from n/a through 2.6.11.	2024-06-08	4.3	CVE-2024-35682
themekraft -- buddyforms	The BuddyForms plugin for WordPress is vulnerable to Email Verification Bypass in all versions up to, and including, 2.8.9 via the use of an insufficiently random activation code. This makes it possible for unauthenticated attackers to bypass the email verification.	2024-06-05	5.3	CVE-2024-5149
themesflat -- themesflat_addons_for_elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themesflat Themesflat Addons For Elementor allows Stored XSS.This issue affects Themesflat Addons For Elementor: from n/a through 2.1.2.	2024-06-04	5.4	CVE-2024-35666
themesflat--Themesflat Addons For Elementor	The Themesflat Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via widget tags in all versions up to, and including, 2.1.1 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.	2024-06-06	6.4	CVE-2024-2922
themesflat--Themesflat Addons For Elementor	The Themesflat Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's TF Group Image, TF Nav Menu, TF Posts, TF Woo Product Grid, TF Accordion, and TF Image Box widgets in all versions up to, and including, 2.1.1 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.	2024-06-06	6.4	CVE-2024-4212
themesflat--Themesflat Addons For Elementor	The Themesflat Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting in several widgets via URL parameters in all versions up to, and including, 2.1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-06	6.4	CVE-2024-4458
themesflat--Themesflat Addons For Elementor	The Themesflat Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widget's titles in all versions up to, and including, 2.1.1 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.	2024-06-06	6.4	CVE-2024-4459
themeum--Tutor LMS eLearning and online course solution	The Tutor LMS - eLearning and online course solution plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.7.1 via the 'attempt_delete' function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Instructor-level access and above, to delete arbitrary quiz attempts.	2024-06-07	4.3	CVE-2024-5438
thimpress--LearnPress WordPress LMS Plugin	The LearnPress - WordPress LMS Plugin plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.2.6.8 due to incorrect implementation of get_items_permissions_check function. This makes it possible for unauthenticated attackers to extract basic information about website users, including their emails	2024-06-05	5.3	CVE-2024-5483

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Tips and Tricks HQ--Stripe Payments	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Tips and Tricks HQ Stripe Payments allows Code Injection.This issue affects Stripe Payments: from n/a through 2.0.79.	2024-06-04	5.3	CVE-2023-48285
TNB Mobile Solutions--Cockpit Software	Inclusion of Sensitive Information in Source Code vulnerability in TNB Mobile Solutions Cockpit Software allows Retrieve Embedded Sensitive Data.This issue affects Cockpit Software: before v0.251.1.	2024-06-05	5.3	CVE-2024-1272
tobiasbg--TablePress Tables in WordPress made easy	The TablePress - Tables in WordPress made easy plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 2.3 via the get_files_to_import() function. This makes it possible for authenticated attackers, with author-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. Due to the complex nature of protecting against DNS rebind attacks in WordPress software, we settled on the developer simply restricting the usage of the URL import functionality to just administrators. While this is not optimal, we feel this poses a minimal risk to most site owners and ideally WordPress core would correct this issue in wp_safe_remote_get() and other functions.	2024-06-07	6.4	CVE-2024-4354
Tomas Cordero--Safety Exit	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Tomas Cordero Safety Exit allows Stored XSS.This issue affects Safety Exit: from n/a through 1.7.0.	2024-06-03	5.9	CVE-2024-35640
UAPP GROUP--Testimonial Carousel For Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in UAPP GROUP Testimonial Carousel For Elementor allows Stored XSS.This issue affects Testimonial Carousel For Elementor: from n/a through 10.1.1.	2024-06-08	6.5	CVE-2024-35713
Unlimited Elements--Unlimited Elements For Elementor (Free Widgets, Addons, Templates)	Missing Authorization vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates).This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 1.5.109.	2024-06-05	4.3	CVE-2024-35674
victorfreitas--WPUpper Share Buttons	The WPUpper Share Buttons plugin for WordPress is vulnerable to unauthorized access of data when preparing sharing links for posts and pages in all versions up to, and including, 3.43. This makes it possible for unauthenticated attackers to obtain the contents of password protected posts and pages.	2024-06-04	5.3	CVE-2024-4997
VideoWhisper--Picture Gallery	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in VideoWhisper Picture Gallery allows Stored XSS.This issue affects Picture Gallery: from n/a through 1.5.11.	2024-06-04	6.5	CVE-2024-34759
visualcomposer --visual_composer_website_builder	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in visualcomposer.Com Visual Composer Website Builder allows Stored XSS.This issue affects Visual Composer Website Builder: from n/a through 45.8.0.	2024-06-04	5.4	CVE-2024-35653
Volkswagen Group Charging GmbH - Elli, EVBox--ID Charger Connect & Pro	An attacker with access to the private network (the charger is connected to) or local access to the Ethernet-Interface can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass	2024-06-06	6.3	CVE-2024-5684

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to bypass the authentication mechanism.			
vollstart -- event_tickets_with_ticket_scanner	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Saso Nikolov Event Tickets with Ticket Scanner allows Reflected XSS.This issue affects Event Tickets with Ticket Scanner: from n/a through 2.3.1.	2024-06-04	6.1	CVE-2024-35652
Vsourz Digital--Responsive Slick Slider WordPress	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Vsourz Digital Responsive Slick Slider WordPress allows Code Injection.This issue affects Responsive Slick Slider WordPress: from n/a through 1.4.	2024-06-04	6.5	CVE-2023-49852
wbcomdesigns--Wbcom Designs Custom Font Uploader	The Wbcom Designs - Custom Font Uploader plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'cfu_delete_customfont' function in all versions up to, and including, 2.3.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete any custom font.	2024-06-06	4.3	CVE-2024-5489
wcmp--MultiVendorX Marketplace WooCommerce MultiVendor Marketplace Solution	The MultiVendorX Marketplace - WooCommerce MultiVendor Marketplace Solution plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'hover_animation' parameter in all versions up to, and including, 4.1.11 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.	2024-06-06	6.4	CVE-2024-5259
web-audimex -- audimexee	Cross Site Scripting vulnerability in audimex audimexEE v.15.1.2 and fixed in 15.1.3.9 allows a remote attacker to execute arbitrary code via the service, method, widget_type, request_id, payload parameters.	2024-06-04	5.4	CVE-2024-30889
WebFactory Ltd--Captcha Code	Improper Restriction of Excessive Authentication Attempts vulnerability in WebFactory Ltd Captcha Code allows Functionality Bypass.This issue affects Captcha Code: from n/a through 2.9.	2024-06-04	5.3	CVE-2023-48745
webfactory--Minimal Coming Soon Coming Soon Page	The Minimal Coming Soon - Coming Soon Page plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the validate_ajax, deactivate_ajax, and save_ajax functions in all versions up to, and including, 2.38. This makes it possible for authenticated attackers, with Subscriber-level access and above, to edit the license key, which could disable features of the plugin.	2024-06-08	6.3	CVE-2024-5087
webfactory--WP Force SSL & HTTPS SSL Redirect	The WP Force SSL & HTTPS SSL Redirect plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ajax_save_setting' function in versions up to, and including, 1.66. This makes it possible for authenticated attackers, subscriber-level permissions and above, to update the plugin settings.	2024-06-08	4.2	CVE-2024-5770
webfactory--WP Reset Most Advanced WordPress Reset Tool	The WP Reset plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the save_ajax function in all versions up to, and including, 2.02. This makes it possible for authenticated attackers, with subscriber-level access and above, to modify the value fo the 'License Key' field for the 'Activate Pro License' setting.	2024-06-08	4.3	CVE-2024-4661
Webliberty--Simple Spoiler	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Webliberty Simple Spoiler allows Stored XSS.This issue affects Simple Spoiler: from n/a through 1.2.	2024-06-03	5.9	CVE-2024-35639

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
westerndeal--CF7 Google Sheets Connector	The CF7 Google Sheets Connector plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'execute_post_data_cg7_free' function in all versions up to, and including, 5.0.9. This makes it possible for unauthenticated attackers to toggle site configuration settings, including WP_DEBUG, WP_DEBUG_LOG, SCRIPT_DEBUG, and SAVEQUERIES.	2024-06-08	6.5	CVE-2024-5654
westguard--WS Form LITE Drag & Drop Contact Form Builder for WordPress	The WS Form LITE plugin for WordPress is vulnerable to CSV Injection in versions up to, and including, 1.9.217. This allows unauthenticated attackers to embed untrusted input into exported CSV files, which can result in code execution when these files are downloaded and opened on a local system with a vulnerable configuration.	2024-06-07	4.7	CVE-2023-5424
willnorris--Open Graph	The Open Graph plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.11.2 via the 'opengraph_default_description' function. This makes it possible for unauthenticated attackers to extract sensitive data including partial content of password-protected blog posts.	2024-06-06	5.3	CVE-2024-5615
wordpresschef--Salon Booking System	The Salon booking system plugin for WordPress is vulnerable to unauthorized access and modification of data due to a missing capability check on several functions hooked into admin_init in all versions up to, and including, 9.9. This makes it possible for authenticated attackers with subscriber access or higher to modify plugin settings and view discount codes intended for other users.	2024-06-08	4.3	CVE-2024-4468
Wow-Company--Woocommerce Recent Purchases	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Wow-Company Woocommerce - Recent Purchases allows PHP Local File Inclusion.This issue affects Woocommerce - Recent Purchases: from n/a through 1.0.1.	2024-06-04	4.9	CVE-2024-35634
WP Darko--Responsive Tabs	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in WP Darko Responsive Tabs allows Code Injection.This issue affects Responsive Tabs: from n/a before 4.0.6.	2024-06-04	5.4	CVE-2023-45635
WP Discussion Board--Discussion Board	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in WP Discussion Board Discussion Board allows Content Spoofing, Cross-Site Scripting (XSS).This issue affects Discussion Board: from n/a through 2.4.8.	2024-06-04	5.4	CVE-2023-39161
WP Hait--Post Grid Elementor Addon	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Hait Post Grid Elementor Addon allows Stored XSS.This issue affects Post Grid Elementor Addon: from n/a through 2.0.16.	2024-06-03	6.5	CVE-2024-34789
WP Moose--Kenta Gutenberg Blocks Responsive Blocks and block templates library for Gutenberg Editor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Moose Kenta Gutenberg Blocks Responsive Blocks and block templates library for Gutenberg Editor allows Stored XSS.This issue affects Kenta Gutenberg Blocks Responsive Blocks and block templates library for Gutenberg Editor: from n/a through 1.3.9.	2024-06-08	6.5	CVE-2024-35731
wpbean--WPB Elementor Addons	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in wpbean WPB Elementor Addons allows Stored XSS.This issue affects WPB Elementor Addons: from n/a through 1.0.9.	2024-06-03	6.5	CVE-2024-34791

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WPBlockArt--BlockArt Blocks	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPBlockArt BlockArt Blocks allows Stored XSS.This issue affects BlockArt Blocks: from n/a through 2.1.5.	2024-06-08	6.5	CVE-2024-35704
wpchill--Strong Testimonials	The Strong Testimonials plugin for WordPress is vulnerable to unauthorized modification of data due to an improper capability check on the wpmtst_save_view_sticky function in all versions up to, and including, 3.1.12. This makes it possible for authenticated attackers, with contributor access and above, to modify favorite views.	2024-06-07	4.3	CVE-2023-6491
WPDeveloper--Essential Addons for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPDeveloper Essential Addons for Elementor allows Stored XSS.This issue affects Essential Addons for Elementor: from n/a through 5.9.15.	2024-06-03	6.5	CVE-2024-34764
wpdevteam--EmbedPress Embed PDF, Google Docs, Vimeo, Wistia, Embed YouTube Videos, Audios, Maps & Embed Any Documents in Gutenberg & Elementor	The EmbedPress - Embed PDF, Google Docs, Vimeo, Wistia, Embed YouTube Videos, Audios, Maps & Embed Any Documents in Gutenberg & Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' attribute within the plugin's EmbedPress PDF widget in all versions up to, and including, 4.0.1 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.	2024-06-05	6.4	CVE-2024-5571
wpdevteam--Essential Addons for Elementor Best Elementor Templates, Widgets, Kits & WooCommerce Builders	The Essential Addons for Elementor - Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'get_manual_calendar_events' function in all versions up to, and including, 5.9.22 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.	2024-06-06	6.4	CVE-2024-5188
wpecommerce--Recurring PayPal Donations	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in wpecommerce Recurring PayPal Donations allows Stored XSS.This issue affects Recurring PayPal Donations: from n/a through 1.7.	2024-06-08	6.5	CVE-2024-35676
WPManageNinja LLC--Ninja Tables	Server-Side Request Forgery (SSRF) vulnerability in WPManageNinja LLC Ninja Tables.This issue affects Ninja Tables: from n/a through 5.0.9.	2024-06-03	4.4	CVE-2024-35635
WPMU DEV--Branda	Authentication Bypass by Spoofing vulnerability in WPMU DEV Branda allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Branda: from n/a through 3.4.14.	2024-06-04	5.3	CVE-2023-51542
WPMU DEV--Defender Security	Improper Authentication vulnerability in WPMU DEV Defender Security allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Defender Security: from n/a through 4.2.0.	2024-06-04	5.3	CVE-2023-47189
wponlinesupport--Album and Image Gallery plus Lightbox	The The Album and Image Gallery plus Lightbox plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 2.0. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	2024-06-06	6.5	CVE-2024-4194

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WPPlugins WordPress Security Plugins--Hide My WP Ghost	Improper Restriction of Excessive Authentication Attempts vulnerability in WPPlugins - WordPress Security Plugins Hide My WP Ghost allows Functionality Bypass.This issue affects Hide My WP Ghost: from n/a through 5.0.25.	2024-06-04	5.3	CVE-2023-34001
wppool--WP Dark Mode WordPress Dark Mode Plugin for Improved Accessibility, Dark Theme, Night Mode, and Social Sharing	The WP Dark Mode - WordPress Dark Mode Plugin for Improved Accessibility, Dark Theme, Night Mode, and Social Sharing plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the wpdm_social_share_save_options function in all versions up to, and including, 5.0.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update the plugin's settings.	2024-06-06	4.3	CVE-2024-5449
wppost--WP-Recall Registration, Profile, Commerce & More	The WP-Recall - Registration, Profile, Commerce & More plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'delete_payment' function in all versions up to, and including, 16.26.6. This makes it possible for unauthenticated attackers to delete arbitrary payments.	2024-06-06	5.3	CVE-2024-1175
wproyal--Royal Elementor Addons and Templates	The Royal Elementor Addons and Templates for WordPress is vulnerable to Stored Cross-Site Scripting via the 'inline_list' parameter in versions up to, and including, 1.3.976 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-07	6.4	CVE-2024-4488
wproyal--Royal Elementor Addons and Templates	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'custom_upload_mimes' function in versions up to, and including, 1.3.976 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-07	6.4	CVE-2024-4489
wpvivid -- wpvivid_backup_for_mainwp	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPvivid Team WPvivid Backup for MainWP allows Reflected XSS.This issue affects WPvivid Backup for MainWP: from n/a through 0.9.32.	2024-06-04	6.1	CVE-2024-35664
wpweaver--Weaver Xtreme Theme Support	The Weaver Xtreme Theme Support plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's div shortcode in all versions up to, and including, 6.4 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.	2024-06-05	6.4	CVE-2024-4939
wpxpo--Post Grid Gutenberg Blocks and WordPress Blog Plugin PostX	The Post Grid Gutenberg Blocks and WordPress Blog Plugin - PostX plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the filterMobileText parameter in all versions up to, and including, 4.0.4 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.	2024-06-08	6.4	CVE-2024-5758
Xabier Miranda--WP Back Button	Cross Site Scripting (XSS) vulnerability in Xabier Miranda WP Back Button allows Stored XSS.This issue affects WP Back Button: from n/a through 1.1.3.	2024-06-03	5.9	CVE-2024-35643
xootix--Login/Signup Popup (Inline	The Login/Signup Popup (Inline Form + Woocommerce) plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'export_settings' function in versions 2.7.1 to 2.7.2. This makes it possible for	2024-06-06	4.3	CVE-2024-5665

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Form + Woocommerce)	authenticated attackers, with Subscriber-level access and above, to read arbitrary options on affected sites.			
YITH--YITH Custom Login	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in YITH YITH Custom Login allows Stored XSS.This issue affects YITH Custom Login: from n/a through 1.7.0.	2024-06-08	5.9	CVE-2024-35732
YITH--YITH WooCommerce Tab Manager	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in YITH YITH WooCommerce Tab Manager allows Stored XSS.This issue affects YITH WooCommerce Tab Manager: from n/a through 1.35.0.	2024-06-08	5.9	CVE-2024-35698
YITH--YITH WooCommerce Wishlist	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in YITH YITH WooCommerce Wishlist allows Stored XSS.This issue affects YITH WooCommerce Wishlist: from n/a through 3.32.0.	2024-06-03	5.9	CVE-2024-34385
yonifre--Maspik Spam blacklist	Authentication Bypass by Spoofing vulnerability in yonifre Maspik - Spam blacklist allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Maspik - Spam blacklist: from n/a through 0.10.3.	2024-06-04	5.3	CVE-2023-48271
zhuyi--BuddyPress Members Only	The BuddyPress Members Only plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.3.5 via the REST API. This makes it possible for unauthenticated attackers to bypass the plugin's "All Other Sections On Your Site Will be Opened to Guest" feature (when unset) and view restricted page and post content.	2024-06-06	5.3	CVE-2024-0972
zootemplate--Clever Addons for Elementor	The Clever Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the CAFE Icon, CAFE Team Member, and CAFE Slider widgets in all versions up to, and including, 2.1.9 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.	2024-06-06	6.4	CVE-2024-2350
3uu--Shariff Wrapper	The Shariff Wrapper plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'shariff' shortcode in all versions up to, and including, 4.6.13 due to insufficient input sanitization and output escaping on user supplied attributes such as 'borderradius' and 'timestamp'. 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.	2024-06-15	6.4	CVE-2024-2695
A WP Life--Album Gallery WordPress Gallery	Missing Authorization vulnerability in A WP Life Album Gallery - WordPress Gallery.This issue affects Album Gallery - WordPress Gallery: from n/a through 1.5.7.	2024-06-10	4.3	CVE-2024-35720
A WP Life--Media Slider Photo Sleder, Video Slider, Link Slider, Carousal Slideshow	Missing Authorization vulnerability in A WP Life Media Slider - Photo Sleder, Video Slider, Link Slider, Carousal Slideshow.This issue affects Media Slider - Photo Sleder, Video Slider, Link Slider, Carousal Slideshow: from n/a through 1.3.9.	2024-06-10	4.3	CVE-2024-35717
acurax -- under_construction_\/_maintenance_mode	Authentication Bypass by Spoofing vulnerability in Acurax Under Construction / Maintenance Mode from Acurax allows Authentication Bypass.This issue affects Under Construction / Maintenance Mode from Acurax: from n/a through 2.6.	2024-06-10	5.3	CVE-2024-35749

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
AddonMaster--Load More Anything	Missing Authorization vulnerability in AddonMaster Load More Anything.This issue affects Load More Anything: from n/a through 3.3.3.	2024-06-11	5.4	CVE-2024-24704
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-20769
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-20784
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-26036
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form.	2024-06-13	5.4	CVE-2024-26037
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability.	2024-06-13	5.4	CVE-2024-26039
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability.	2024-06-13	5.4	CVE-2024-26053
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-26054
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the malicious script.	2024-06-13	5.4	CVE-2024-26055
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that triggers the malicious script.	2024-06-13	5.4	CVE-2024-26057
adobe -- experience_manag	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow	2024-06-13	5.4	CVE-2024-26058

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
er	an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link.			
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-26060
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-26066
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-26068
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-26070
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-26071
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that causes the vulnerable script to execute.	2024-06-13	5.4	CVE-2024-26072
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-26074
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-26075
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-26077
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-26078
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-26081
adobe -- experience_manag	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject	2024-06-13	5.4	CVE-2024-26082

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
er	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.			
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-26083
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-26085
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-26088
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-26092
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-06-13	5.4	CVE-2024-26093
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-26095
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-26110
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-06-13	5.4	CVE-2024-26111
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-06-13	5.4	CVE-2024-26113
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-06-13	5.4	CVE-2024-26114
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-06-13	5.4	CVE-2024-26115
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-06-13	5.4	CVE-2024-26116

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-26121
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-26123
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-34119
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-34120
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 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.	2024-06-13	5.4	CVE-2024-36141
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36142
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36143
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36144
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36146
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36147
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36148
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36149
adobe -- experience_manag	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject	2024-06-13	5.4	CVE-2024-36150

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
er	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.			
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36152
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36153
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36154
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36155
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36156
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36158
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36159
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36160
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36161
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36162
adobe -- experience_manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a 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.	2024-06-13	4.8	CVE-2024-26049
Adobe--Acrobat Mobile Sign	Acrobat Mobile Sign Android versions 24.4.2.33155 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in a security feature bypass. An attacker could exploit this vulnerability to access files and directories that are outside the restricted	2024-06-13	6.3	CVE-2024-34129

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Android	directory and also to overwrite arbitrary files. Exploitation of this issue does not requires user interaction and attack complexity is high.			
Adobe--Acrobat Mobile Sign Android	Acrobat Mobile Sign Android versions 24.4.2.33155 and earlier are affected by an Incorrect Authorization vulnerability that could result in a Security feature bypass. An attacker could exploit this vulnerability to access confidential information. Exploitation of this issue does not require user interaction.	2024-06-13	5.5	CVE-2024-34130
Adobe--Adobe Commerce	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could result in arbitrary code execution. An attacker could exploit this vulnerability by sending a crafted request to the server, which could then cause the server to execute arbitrary code. Exploitation of this issue does not require user interaction.	2024-06-13	6.5	CVE-2024-34111
Adobe--Adobe Commerce	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. An attacker could exploit this vulnerability to gain unauthorized access or perform actions with the privileges of another user. Exploitation of this issue does not require user interaction.	2024-06-13	5.3	CVE-2024-34106
Adobe--Adobe Commerce	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized access. Exploitation of this issue does not require user interaction.	2024-06-13	5.3	CVE-2024-34107
Adobe--Adobe Commerce	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 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 vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-06-13	4.8	CVE-2024-34105
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-06-13	5.4	CVE-2024-26086
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, as the victim needs to visit a web page with a maliciously crafted script.	2024-06-13	5.4	CVE-2024-26089
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link.	2024-06-13	5.4	CVE-2024-26090
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that causes the vulnerable script to execute.	2024-06-13	5.4	CVE-2024-26091
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-06-13	5.4	CVE-2024-26117

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, as the victim needs to visit a web page with a maliciously crafted script.	2024-06-13	5.4	CVE-2024-36151
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36157
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36163
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36164
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36165
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36166
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36167
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36168
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36169
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36170
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36171
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36172
Adobe--Adobe Experience	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject	2024-06-13	5.4	CVE-2024-36173

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Manager	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.			
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36174
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36175
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36176
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36177
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36178
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36179
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36180
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, typically in the form of convincing a victim to visit a maliciously crafted web page or to interact with a maliciously modified DOM element within the application.	2024-06-13	5.4	CVE-2024-36181
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36182
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form.	2024-06-13	5.4	CVE-2024-36183
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a malicious link or to submit a specially crafted form.	2024-06-13	5.4	CVE-2024-36184

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36185
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36186
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36187
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36188
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36189
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that triggers the vulnerability.	2024-06-13	5.4	CVE-2024-36190
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36191
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36192
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36193
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36194
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36195
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36196

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability.	2024-06-13	5.4	CVE-2024-36197
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36198
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36199
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36200
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36201
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36202
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36203
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36204
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36205
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-06-13	5.4	CVE-2024-36206
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36207
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36208

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36209
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-06-13	5.4	CVE-2024-36210
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-06-13	5.4	CVE-2024-36211
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36212
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36213
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36214
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36215
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-06-13	5.4	CVE-2024-36216
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36217
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36218
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36219
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the malicious script.	2024-06-13	5.4	CVE-2024-36220

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36221
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability.	2024-06-13	5.4	CVE-2024-36222
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the vulnerable script to execute.	2024-06-13	5.4	CVE-2024-36224
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-06-13	5.4	CVE-2024-36225
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form.	2024-06-13	5.4	CVE-2024-36227
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability.	2024-06-13	5.4	CVE-2024-36228
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form.	2024-06-13	5.4	CVE-2024-36229
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the execution of the malicious script.	2024-06-13	5.4	CVE-2024-36230
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the execution of the malicious script.	2024-06-13	5.4	CVE-2024-36231
Adobe--Adobe Experience	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject	2024-06-13	5.4	CVE-2024-36232

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Manager	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.			
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a malicious link.	2024-06-13	5.4	CVE-2024-36233
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that triggers the vulnerability.	2024-06-13	5.4	CVE-2024-36234
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the execution of the malicious script.	2024-06-13	5.4	CVE-2024-36235
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link.	2024-06-13	5.4	CVE-2024-36236
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a malicious link or to interact with a maliciously crafted web page.	2024-06-13	5.4	CVE-2024-36238
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link.	2024-06-13	5.4	CVE-2024-36239
Adobe--Audition	Audition versions 24.2, 23.6.4 and earlier Answer: 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.	2024-06-13	5.5	CVE-2024-30276
Adobe--Audition	Audition versions 24.2, 23.6.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service condition. An attacker could exploit this vulnerability to crash the application, leading to a denial of service. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-06-13	5.5	CVE-2024-30285
Adobe--ColdFusion	ColdFusion versions 2023u7, 2021u13 and earlier are affected by a Weak Cryptography for Passwords vulnerability that could result in a security feature bypass. This vulnerability arises due to the use of insufficiently strong cryptographic algorithms or flawed implementation that compromises the confidentiality of password data. An attacker could exploit this weakness to decrypt or guess passwords, potentially gaining unauthorized access to protected resources. Exploitation of this issue does not require user interaction.	2024-06-13	6.2	CVE-2024-34113

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Adobe--Creative Cloud Desktop	Creative Cloud Desktop versions 6.1.0.587 and earlier are affected by an Uncontrolled Search Path Element vulnerability that could result in a security feature bypass. An attacker could exploit this vulnerability to load and execute malicious libraries, leading to arbitrary file delete. Exploitation of this issue requires user interaction.	2024-06-13	5.5	CVE-2024-34116
Adobe--Media Encoder	Media Encoder versions 23.6.5, 24.3 and earlier Answer: 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.	2024-06-13	5.5	CVE-2024-30278
Afzal Multani--WP Clone Menu	Missing Authorization vulnerability in Afzal Multani WP Clone Menu.This issue affects WP Clone Menu: from n/a through 1.0.1.	2024-06-12	5.4	CVE-2023-38395
aimeos--ai-client-html	The Aimeos HTML client provides Aimeos HTML components for e-commerce projects. Starting in version 2020.04.1 and prior to versions 2020.10.27, 2021.10.21, 2022.10.12, 2023.10.14, and 2024.04.5, digital downloads sold in online shops can be downloaded without valid payment, e.g. if the payment didn't succeed. Versions 2020.10.27, 2021.10.21, 2022.10.12, 2023.10.14, and 2024.04.5 fix this issue.	2024-06-11	5.3	CVE-2024-37296
aimeos--aimeos-core	Aimeos is an Open Source e-commerce framework for online shops. All SaaS and marketplace setups using Aimeos version from 2022/2023/2024 are affected by a potential denial of service attack. Users should upgrade to versions 2022.10.17, 2023.10.17, or 2024.04 of the aimeos/aimeos-core package to receive a patch.	2024-06-11	5.5	CVE-2024-37294
Anders Norn--Radcliffe 2	Missing Authorization vulnerability in Anders NorÃ©n Radcliffe 2.This issue affects Radcliffe 2: from n/a through 2.0.17.	2024-06-11	5.3	CVE-2024-35685
apple -- macos	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in macOS Monterey 12.5. A website may be able to track the websites a user visited in Safari private browsing mode.	2024-06-10	5.3	CVE-2022-32933
apple -- macos	The issue was addressed with improved restriction of data container access. This issue is fixed in macOS Ventura 13.6.5, macOS Monterey 12.7.4. An app may be able to access sensitive user data.	2024-06-10	5.5	CVE-2023-40389
apple -- macos	This issue was addressed by adding an additional prompt for user consent. This issue is fixed in macOS Sonoma 14.4. An app may be able to access user-sensitive data.	2024-06-10	5.5	CVE-2024-27792
Aspose.cloud Marketplace--Aspose.Words Exporter	Missing Authorization vulnerability in Aspose.Cloud Marketplace Aspose.Words Exporter.This issue affects Aspose.Words Exporter: from n/a through 6.3.1.	2024-06-11	4.3	CVE-2024-32146
ASUS--Download Master	The parameter used in the certain page of ASUS Download Master is not properly filtered for user input. A remote attacker with administrative privilege can insert JavaScript code to the parameter for Reflected Cross-site scripting attacks.	2024-06-14	4.8	CVE-2024-31159
ASUS--Download Master	The parameter used in the certain page of ASUS Download Master is not properly filtered for user input. A remote attacker with administrative privilege can insert JavaScript code to the parameter for Stored Cross-site scripting attacks.	2024-06-14	4.8	CVE-2024-31160
Awesome Support Team--Awesome Support	Missing Authorization vulnerability in Awesome Support Team Awesome Support.This issue affects Awesome Support: from n/a through 6.1.5.	2024-06-12	5.3	CVE-2023-51537

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
baden03--Collapse-O-Matic	The Collapse-O-Matic plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'expand' and 'expandsub' shortcode in all versions up to, and including, 1.8.5.7 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.	2024-06-15	6.4	CVE-2024-4095
badhonrocks--Divi Torque Lite Divi Theme and Extra Theme	The Divi Torque Lite - Divi Theme and Extra Theme plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'support_unfiltered_files_upload' function in all versions up to, and including, 3.6.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-12	6.4	CVE-2024-5892
Bastianon Massimo--WP GPX Map	Missing Authorization vulnerability in Bastianon Massimo WP GPX Map.This issue affects WP GPX Map: from n/a through 1.7.08.	2024-06-12	4.3	CVE-2023-44234
BBS e-Theme--BBS e-Popup	Missing Authorization vulnerability in BBS e-Theme BBS e-Popup.This issue affects BBS e-Popup: from n/a through 2.4.5.	2024-06-14	6.5	CVE-2023-36504
bdthemes--Element Pack Elementor Addons (Header Footer, Template Library, Dynamic Grid & Carousel, Remote Arrows)	The Element Pack Elementor Addons (Header Footer, Template Library, Dynamic Grid & Carousel, Remote Arrows) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Creative Button widget in all versions up to, and including, 5.6.7 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.	2024-06-12	6.4	CVE-2024-3925
BeyondTrust--BeyondInsight PasswordSafe	A medium severity vulnerability in BIPS has been identified where an authenticated attacker with high privileges can access the SSH private keys via an information leak in the server response.	2024-06-11	5.9	CVE-2024-5813
bradvin--FooGallery Responsive Photo Gallery, Image Viewer, Justified, Masonry & Carousel	The Best WordPress Gallery Plugin - FooGallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via album gallery custom URLs in all versions up to, and including, 2.4.15 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.	2024-06-14	6.4	CVE-2024-2122
Brainstorm Force--ProjectHuddle Client Site	Missing Authorization vulnerability in Brainstorm Force ProjectHuddle Client Site.This issue affects ProjectHuddle Client Site: from n/a through 1.0.34.	2024-06-14	4.3	CVE-2023-51376
brainstormforce--Elementor Header & Footer Builder	The Elementor Header & Footer Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the url attribute within the plugin's Site Title widget in all versions up to, and including, 1.6.35 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.	2024-06-13	6.4	CVE-2024-5757

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Brett Shumaker--Simple Staff List	Missing Authorization vulnerability in Brett Shumaker Simple Staff List.This issue affects Simple Staff List: from n/a through 2.2.4.	2024-06-12	4.3	CVE-2023-51526
britner--Gutenberg Blocks with AI by Kadence WP Page Builder Features	The Gutenberg Blocks with AI by Kadence WP - Page Builder Features plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'titleFont' parameter in all versions up to, and including, 3.2.38 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.	2024-06-14	6.4	CVE-2024-4863
Bryan Lee--Kingkong Board	Missing Authorization vulnerability in Bryan Lee Kingkong Board.This issue affects Kingkong Board: from n/a through 2.1.0.2.	2024-06-14	6.3	CVE-2023-36694
buddypress--BuddyPress	The BuddyPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'display_name' parameter in versions up to, and including, 12.4.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-12	6.4	CVE-2024-4892
BulkGate--BulkGate SMS Plugin for WooCommerce	Missing Authorization vulnerability in BulkGate BulkGate SMS Plugin for WooCommerce.This issue affects BulkGate SMS Plugin for WooCommerce: from n/a through 3.0.2.	2024-06-12	5.4	CVE-2023-51679
Business Directory Team--Business Directory Plugin	Missing Authorization vulnerability in Business Directory Team Business Directory Plugin.This issue affects Business Directory Plugin: from n/a through 6.3.9.	2024-06-14	5.4	CVE-2023-51516
Buy Me a Coffee--Buy Me a Coffee	Missing Authorization vulnerability in Buy Me a Coffee.This issue affects Buy Me a Coffee: from n/a through 3.7.	2024-06-12	4.3	CVE-2023-25030
Code for Recovery--12 Step Meeting List	Missing Authorization vulnerability in Code for Recovery 12 Step Meeting List.This issue affects 12 Step Meeting List: from n/a through 3.14.28.	2024-06-10	4.3	CVE-2024-22296
Codection--Import and export users and customers	Missing Authorization vulnerability in Codection Import and export users and customers.This issue affects Import and export users and customers: from n/a through 1.26.5.	2024-06-11	5.4	CVE-2024-34815
codename065--Download Manager	The Download Manager Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via wpdm_user_dashboard, wpdm_package, wpdm_packages, wpdm_search_result, and wpdm_tag shortcodes in all versions up to, and including, 3.2.92 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.	2024-06-12	6.4	CVE-2024-5266

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
codename065--Download Manager	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via a user's Display Name in all versions up to, and including, 3.2.86 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. This vulnerability requires social engineering to successfully exploit, and the impact would be very limited due to the attacker requiring a user to login as the user with the injected payload for execution.	2024-06-12	4.4	CVE-2024-1766
codexpert--CoDesigner The Most Compact and User-Friendly Elementor WooCommerce Builder	The CoDesigner WooCommerce Builder for Elementor - Customize Checkout, Shop, Email, Products & More plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Shop Slider, Tabs Classic, and Image Comparison widgets in all versions up to, and including, 4.4.1 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.	2024-06-12	6.4	CVE-2024-4564
Comtrend--Comtrend WLD71-T1_v2.0.201820	Cross-Site Request Forgery vulnerability in Comtrend router WLD71-T1_v2.0.201820, affecting the GRG-4280us version. This vulnerability allows an attacker to force an end user to execute unwanted actions in a web application to which he is authenticated.	2024-06-10	6.5	CVE-2024-5786 cve-
Contact List PRO--Contact List Easy Business Directory, Staff Directory and Address Book Plugin	Missing Authorization vulnerability in Contact List PRO Contact List - Easy Business Directory, Staff Directory and Address Book Plugin.This issue affects Contact List - Easy Business Directory, Staff Directory and Address Book Plugin: from n/a through 2.9.87.	2024-06-11	5.3	CVE-2024-34821
contact_form_builder_project --contact_form_builder	Improper Restriction of Excessive Authentication Attempts vulnerability in wpdevart Contact Form Builder, Contact Widget allows Functionality Bypass.This issue affects Contact Form Builder, Contact Widget: from n/a through 2.1.7.	2024-06-10	5.3	CVE-2024-35747
Copymatic--Copymatic AI Content Writer & Generator	Missing Authorization vulnerability in Copymatic Copymatic - AI Content Writer & Generator.This issue affects Copymatic - AI Content Writer & Generator: from n/a through 1.9.	2024-06-11	6.5	CVE-2024-35716
crate--crate	CrateDB is a distributed SQL database. A high-risk vulnerability has been identified in versions prior to 5.7.2 where the TLS endpoint (port 4200) permits client-initiated renegotiation. In this scenario, an attacker can exploit this feature to repeatedly request renegotiation of security parameters during an ongoing TLS session. This flaw could lead to excessive consumption of CPU resources, resulting in potential server overload and service disruption. The vulnerability was confirmed using an openssl client where the command `R` initiates renegotiation, followed by the server confirming with `RENEGOTIATING`. This vulnerability allows an attacker to perform a denial of service attack by exhausting server CPU resources through repeated TLS renegotiations. This impacts the availability of services running on the affected server, posing a significant risk to operational stability and security. TLS 1.3 explicitly forbids renegotiation, since it closes a window of opportunity for an attack. Version 5.7.2 of CrateDB contains the fix for the issue.	2024-06-13	5.3	CVE-2024-37309

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Deepak anand--WP Dummy Content Generator	Missing Authorization vulnerability in Deepak anand WP Dummy Content Generator.This issue affects WP Dummy Content Generator: from n/a through 2.3.0.	2024-06-14	5.3	CVE-2023-37394
Dell--CPG BIOS	Dell Client Platform contains an incorrect authorization vulnerability. An attacker with physical access to the system could potentially exploit this vulnerability by bypassing BIOS authorization to modify settings in the BIOS.	2024-06-12	6.8	CVE-2024-0160
Dell--CPG BIOS	Dell Client Platform BIOS contains an Improper Input Validation vulnerability in an externally developed component. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	2024-06-13	5.1	CVE-2024-32856
Dell--CPG BIOS	Dell Client BIOS contains an Out-of-bounds Write vulnerability. A local authenticated malicious user with admin privileges could potentially exploit this vulnerability, leading to platform denial of service.	2024-06-12	4.7	CVE-2024-28970
Dell--Secure Connect Gateway-Application	Dell SCG, versions prior to 5.24.00.00, contain an Improper Access Control vulnerability in the SCG exposed for an internal enable REST API (if enabled by Admin user from UI). A remote low privileged attacker could potentially exploit this vulnerability, leading to the execution of certain Internal APIs applicable only for Admin Users on the application's backend database that could potentially allow an unauthorized user access to restricted resources and change of state.	2024-06-13	5.4	CVE-2024-28965
Dell--Secure Connect Gateway-Application	Dell SCG, versions prior to 5.24.00.00, contain an Improper Access Control vulnerability in the SCG exposed for an internal update REST API (if enabled by Admin user from UI). A remote low privileged attacker could potentially exploit this vulnerability, leading to the execution of certain APIs applicable only for Admin Users on the application's backend database that could potentially allow an unauthorized user access to restricted resources and change of state.	2024-06-13	5.4	CVE-2024-28966
Dell--Secure Connect Gateway-Application	Dell SCG, versions prior to 5.24.00.00, contain an Improper Access Control vulnerability in the SCG exposed for an internal maintenance REST API (if enabled by Admin user from UI). A remote low privileged attacker could potentially exploit this vulnerability, leading to the execution of certain APIs applicable only for Admin Users on the application's backend database that could potentially allow an unauthorized user access to restricted resources and change of state.	2024-06-13	5.4	CVE-2024-28967
Dell--Secure Connect Gateway-Application	Dell SCG, versions prior to 5.24.00.00, contain an Improper Access Control vulnerability in the SCG exposed for internal email and collection settings REST APIs (if enabled by Admin user from UI). A remote low privileged attacker could potentially exploit this vulnerability, leading to the execution of certain APIs applicable only for Admin Users on the application's backend database that could potentially allow an unauthorized user access to restricted resources and change of state.	2024-06-13	5.4	CVE-2024-28968
Dell--Secure Connect Gateway-Application	Dell SCG, versions prior to 5.22.00.00, contain a SQL Injection Vulnerability in the SCG UI for an internal assets REST API. A remote authenticated attacker could potentially exploit this vulnerability, leading to the execution of certain SQL commands on the application's backend database causing potential unauthorized access and modification of application data.	2024-06-13	5.4	CVE-2024-29168
Dell--Secure Connect Gateway-Application	Dell SCG, versions prior to 5.22.00.00, contain a SQL Injection Vulnerability in the SCG UI for an internal audit REST API. A remote authenticated attacker could potentially exploit this vulnerability, leading to the execution of certain SQL commands on the application's backend database causing potential unauthorized access and modification of application data.	2024-06-13	5.4	CVE-2024-29169
Dell--Secure Connect Gateway-	Dell SCG, versions prior to 5.24.00.00, contain an Improper Access Control vulnerability in the SCG exposed for an internal update REST API (if enabled by Admin user from UI). A remote low privileged attacker could potentially exploit this vulnerability, leading to the execution of certain APIs applicable only for Admin	2024-06-13	4.3	CVE-2024-28969

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Application	Users on the application's backend database that could potentially allow an unauthorized user access to restricted resources.			
devitemsllc--ShopLentor WooCommerce Builder for Elementor & Gutenberg +12 Modules All in One Solution (formerly WooLentor)	The ShopLentor - WooCommerce Builder for Elementor & Gutenberg +12 Modules - All in One Solution (formerly WooLentor) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's WL: Product Horizontal Filter widget in all versions up to, and including, 2.9.0 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.	2024-06-11	6.4	CVE-2024-5530
dgwyer--Simple Sitemap Create a Responsive HTML Sitemap	The Simple Sitemap - Create a Responsive HTML Sitemap plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.5.13. This is due to missing or incorrect nonce validation in the 'admin_notices' hook found in class-settings.php. This makes it possible for unauthenticated attackers to reset the plugin options to a default state via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-06-14	4.3	CVE-2023-6492
Discourse--WP Discourse	Missing Authorization vulnerability in Discourse WP Discourse.This issue affects WP Discourse: from n/a through 2.5.1.	2024-06-11	4.3	CVE-2024-35168
Elastic--Elasticsearch	It was identified that if a cross-cluster API key https://www.elastic.co/guide/en/elasticsearch/reference/8.14/security-api-create-cross-cluster-api-key.html#security-api-create-cross-cluster-api-key-request-body Â restricts search for a given index using the queryÂ or the field_securityÂ parameter, and the same cross-cluster API key also grants replication for the same index, the search restrictions are not enforced during cross cluster search operations and search results may include documents and terms that should not be returned. This issue only affects the API key based security model for remote clusters https://www.elastic.co/guide/en/elasticsearch/reference/8.14/remote-clusters.html#remote-clusters-security-models Â that was previously a beta feature and is released as GA with 8.14.0	2024-06-12	6.5	CVE-2024-23445
Elastic--Elasticsearch	A flaw was discovered in Elasticsearch, affecting document ingestion when an index template contains a dynamic field mapping of "passthrough" type. Under certain circumstances, ingesting documents in this index would cause a StackOverflow exception to be thrown and ultimately lead to a Denial of Service. Note that passthrough fields is an experimental feature.	2024-06-13	4.9	CVE-2024-37280
Elastic--Kibana	An open redirect issue was discovered in Kibana that could lead to a user being redirected to an arbitrary website if they use a maliciously crafted Kibana URL.	2024-06-14	6.1	CVE-2024-23442
Elastic--Kibana	A flaw was discovered in Kibana, allowing view-only users of alerting to use the run_soon API making the alerting rule run continuously, potentially affecting the system availability if the alerting rule is running complex queries.	2024-06-13	4.3	CVE-2024-37279
Elementor--Elementor Website Builder	Missing Authorization vulnerability in Elementor Elementor Website Builder.This issue affects Elementor Website Builder: from n/a through 3.13.2.	2024-06-11	4.3	CVE-2023-33922
elespare--Elespare News, Magazine and Blog Elements & Blog Addons for Elementor with Header Footer	The Elespare - Blog, Magazine and Newspaper Addons for Elementor with Templates, Widgets, Kits, and Header/Footer Builder. One Click Import: No Coding Required! plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Horizontal Nav Menu' widget in all versions up to, and including, 3.1.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and	2024-06-13	6.4	CVE-2024-4615

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Builder. One Click Import: No Coding Required!	above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
emlog -- emlog	Emlog pro2.3 is vulnerable to Cross Site Request Forgery (CSRF) via twitter.php which can be used with a XSS vulnerability to access administrator information.	2024-06-10	6.5	CVE-2024-31612
ExpressTech--Quiz And Survey Master	Missing Authorization vulnerability in ExpressTech Quiz And Survey Master.This issue affects Quiz And Survey Master: from n/a through 8.1.16.	2024-06-14	5.3	CVE-2023-51507
Fastly--Fastly	Missing Authorization vulnerability in Fastly.This issue affects Fastly: from n/a through 1.2.25.	2024-06-11	5.3	CVE-2024-34768
Fat Rat--Fat Rat Collect	Missing Authorization vulnerability in Fat Rat Fat Rat Collect.This issue affects Fat Rat Collect: from n/a through 2.6.7.	2024-06-14	4.3	CVE-2023-35045
Fortinet--FortiOS	A stack-based buffer overflow in Fortinet FortiOS version 7.4.0 through 7.4.1 and 7.2.0 through 7.2.7 and 7.0.0 through 7.0.12 and 6.4.6 through 6.4.15 and 6.2.9 through 6.2.16 and 6.0.13 through 6.0.18 allows attacker to execute unauthorized code or commands via specially crafted CLI commands.	2024-06-11	6.7	CVE-2023-46720
Fortinet--FortiOS	A use of password hash with insufficient computational effort vulnerability [CWE-916] affecting FortiOS version 7.4.3 and below, 7.2 all versions, 7.0 all versions, 6.4 all versions and FortiProxy version 7.4.2 and below, 7.2 all versions, 7.0 all versions, 2.0 all versions may allow aÂ privileged attacker with super-admin profile and CLI access to decrypting the backup file.	2024-06-11	6.8	CVE-2024-23111
Fortinet--FortiPortal	A improper neutralization of special elements used in an sql command ('sql injection') in Fortinet FortiPortal versions 7.0.0 through 7.0.6 and version 7.2.0 allows privileged user to obtain unauthorized information via the report download functionality.	2024-06-11	4.3	CVE-2024-31495
Fortinet--FortiSOAR	Multiple improper neutralization of special elements used inÂ SQL commands ('SQL Injection') vulnerabilities [CWE-89] in FortiSOARÂ 7.2.0 and before 7.0.3 may allow an authenticated attacker to execute unauthorized code or commands via specifically crafted strings parameters.	2024-06-11	6.5	CVE-2023-23775
FunnelKit--FunnelKit Checkout	Missing Authorization vulnerability in FunnelKit FunnelKit Checkout.This issue affects FunnelKit Checkout: from n/a through 3.10.3.	2024-06-12	5.4	CVE-2023-51671
FunnelKit--FunnelKit Checkout	Missing Authorization vulnerability in FunnelKit FunnelKit Checkout.This issue affects FunnelKit Checkout: from n/a through 3.10.3.	2024-06-12	4.3	CVE-2023-51670
futuriowp--Futurio Extra	The Futurio Extra plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'header_size' attribute within the Advanced Text Block widget in all versions up to, and including, 2.0.5 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.	2024-06-11	6.4	CVE-2024-5646
galdub--Folders Unlimited Folders to Organize Media Library Folder, Pages, Posts, File	The Folders and Folders Pro plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 3.0 in Folders and 3.0.2 in Folders Pro via the 'handle_folders_file_upload' function. This makes it possible for authenticated attackers, with author access and above, to upload files to arbitrary locations on the server.	2024-06-14	4.3	CVE-2024-2023

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Manager				
Gangesh Matta--Simple Org Chart	Missing Authorization vulnerability in Gangesh Matta Simple Org Chart.This issue affects Simple Org Chart: from n/a through 2.3.4.	2024-06-12	5.3	CVE-2023-40603
GitLab--GitLab	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.1 prior to 16.10.7, starting from 16.11 prior to 16.11.4, and starting from 17.0 prior to 17.0.2. It was possible for an attacker to cause a denial of service using maliciously crafted file.	2024-06-12	6.5	CVE-2024-1495
GitLab--GitLab	An issue has been discovered in GitLab CE/EE affecting all versions prior to 16.10.7, starting from 16.11 prior to 16.11.4, and starting from 17.0 prior to 17.0.2. A vulnerability in GitLab's CI/CD pipeline editor could allow for denial of service attacks through maliciously crafted configuration files.	2024-06-12	6.5	CVE-2024-1736
GitLab--GitLab	An issue has been discovered in GitLab CE/EE affecting all versions starting from 8.4 prior to 16.10.7, starting from 16.11 prior to 16.11.4, and starting from 17.0 prior to 17.0.2. A vulnerability in GitLab's Asana integration allowed an attacker to potentially cause a regular expression denial of service by sending specially crafted requests.	2024-06-12	6.5	CVE-2024-1963
GitLab--GitLab	A cross-site scripting issue has been discovered in GitLab affecting all versions starting from 5.1 before 16.10.7, all versions starting from 16.11 before 16.111.4, all versions starting from 17.0 before 17.0.2. When viewing an XML file in a repository in raw mode, it can be made to render as HTML if viewed under specific circumstances.	2024-06-12	4.4	CVE-2024-4201
gloriafood--Restaurant Menu Food Ordering System Table Reservation	The Restaurant Menu - Food Ordering System - Table Reservation plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 2.4.0 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.	2024-06-15	6.4	CVE-2024-1399
gpriday--SiteOrigin Widgets Bundle	The SiteOrigin Widgets Bundle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's SiteOrigin Blog Widget in all versions up to, and including, 1.61.1 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.	2024-06-11	6.4	CVE-2024-5090
grpc--grpc-node	@grpc/grps-js implements the core functionality of gRPC purely in JavaScript, without a C++ addon. Prior to versions 1.10.9, 1.9.15, and 1.8.22, there are two separate code paths in which memory can be allocated per message in excess of the `grpc.max_receive_message_length` channel option: If an incoming message has a size on the wire greater than the configured limit, the entire message is buffered before it is discarded; and/or if an incoming message has a size within the limit on the wire but decompresses to a size greater than the limit, the entire message is decompressed into memory, and on the server is not discarded. This has been patched in versions 1.10.9, 1.9.15, and 1.8.22.	2024-06-10	5.3	CVE-2024-37168
HahnCreativeGroup--WP Translate	Missing Authorization vulnerability in HahnCreativeGroup WP Translate.This issue affects WP Translate: from n/a through 5.3.0.	2024-06-11	5.4	CVE-2024-35663
Happyforms--Happyforms	Missing Authorization vulnerability in Happyforms.This issue affects Happyforms: from n/a through 1.25.10.	2024-06-11	5.3	CVE-2024-23521

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Harbor--Harbor	Open Redirect in HarborÂ <=v2.8.4, <=v2.9.2, and <=v2.10.0 may redirect a user to a malicious site.	2024-06-10	4.3	CVE-2024-22244
Hardik Chavada--Sticky Social Media Icons	Missing Authorization vulnerability in Hardik Chavada Sticky Social Media Icons.This issue affects Sticky Social Media Icons: from n/a through 2.1.	2024-06-12	5.4	CVE-2023-40672
Himalaya Saxena--Highcompress Image Compressor	Missing Authorization vulnerability in Himalaya Saxena Highcompress Image Compressor.This issue affects Highcompress Image Compressor: from n/a through 6.0.0.	2024-06-12	6.5	CVE-2023-40209
hiroaki-miyashita--Custom Field Template	The Custom Field Template plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'cpt' shortcode in all versions up to, and including, 2.6.1 due to insufficient input sanitization and output escaping on user supplied post meta. 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.	2024-06-11	6.4	CVE-2023-6745
hiroaki-miyashita--Custom Field Template	The Custom Field Template plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's custom field name column in all versions up to, and including, 2.6.1 due to insufficient input sanitization and output escaping on user supplied custom fields. 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.	2024-06-11	6.4	CVE-2024-0627
hiroaki-miyashita--Custom Field Template	The Custom Field Template plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.6.1 via the 'cft' shortcode. This makes it possible for authenticated attackers with contributor access and above, to extract sensitive data including arbitrary post metadata.	2024-06-11	4.3	CVE-2023-6748
hiroaki-miyashita--Custom Field Template	The Custom Field Template plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.6.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2024-06-11	4.4	CVE-2024-0653
Hitachi Energy--FOXMAN-UN	A vulnerability exists in the FOXMAN-UN/UNEM server / APIGateway that if exploited allows a malicious user to perform an arbitrary number of authentication attempts using different passwords, and eventually gain access to the targeted account.	2024-06-11	6.5	CVE-2024-28022
Hitachi Energy--FOXMAN-UN	A vulnerability exists in the message queueing mechanism that if exploited can lead to the exposure of resources or functionality to unintended actors, possibly providing attackers with sensitive information or even execute arbitrary code.	2024-06-11	5.7	CVE-2024-28023
Huawei--HarmonyOS	Vulnerability of unauthorized screenshot capturing in the WMS module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2024-06-14	6.8	CVE-2024-36499
Huawei--HarmonyOS	Memory management vulnerability in the boottime module Impact: Successful exploitation of this vulnerability can affect integrity.	2024-06-14	5.6	CVE-2024-36501
Huawei--HarmonyOS	Function vulnerabilities in the Calendar module Impact: Successful exploitation of this vulnerability will affect availability.	2024-06-14	5.9	CVE-2024-5465

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Huawei--HarmonyOS	Vulnerability of insufficient permission verification in the NearLink module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2024-06-14	4	CVE-2024-5464
ibericode--MC4WP	Missing Authorization vulnerability in ibericode MC4WP.This issue affects MC4WP: from n/a through 4.9.9.	2024-06-11	5.3	CVE-2023-51682
IBM--Db2 for Linux, UNIX and Windows	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to a denial of service as the server may crash when using a specially crafted query on certain columnar tables by an authenticated user. IBM X-Force ID: 287613.	2024-06-12	6.5	CVE-2024-31881
IBM--Db2 for Linux, UNIX and Windows	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5is vulnerable to a denial of service, under specific configurations, as the server may crash when using a specially crafted SQL statement by an authenticated user. IBM X-Force ID: 287612.	2024-06-12	5.3	CVE-2023-29267
IBM--Db2 for Linux, UNIX and Windows	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query under certain conditions. IBM X-Force ID: 285246.	2024-06-12	5.3	CVE-2024-28762
IBM--Jazz Reporting Service	IBM Jazz Reporting Service 7.0.3 stores user credentials in plain clear text which can be read by an admin user. IBM X-Force ID: 283363.	2024-06-13	4.4	CVE-2024-25052
IBM--Maximo Application Suite	IBM Maximo Asset Management 7.6.1.3 and IBM Maximo Application Suite 8.10 and 8.11 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 279973.	2024-06-13	4	CVE-2024-22333
ideaboxcreations--PowerPack Addons for Elementor (Free Widgets, Extensions and Templates)	The PowerPack Addons for Elementor (Free Widgets, Extensions and Templates) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' attribute within the plugin's Link Effects widget in all versions up to, and including, 2.7.20 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.	2024-06-13	6.4	CVE-2024-5787
If So Plugin--If-So Dynamic Content Personalization	Missing Authorization vulnerability in If So Plugin If-So Dynamic Content Personalization.This issue affects If-So Dynamic Content Personalization: from n/a through 1.7.1.	2024-06-11	6.5	CVE-2024-34820
itsourcecode--Document Management System	A vulnerability classified as critical has been found in itsourcecode Document Management System 1.0. Affected is an unknown function of the file edithis.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-268722 is the identifier assigned to this vulnerability.	2024-06-15	6.3	CVE-2024-6014
itsourcecode--Event Calendar	A vulnerability has been found in itsourcecode Event Calendar 1.0 and classified as critical. Affected by this vulnerability is the function regConfirm/regDelete of the file process.php. The manipulation of the argument userId 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-268699.	2024-06-15	6.3	CVE-2024-6009
itsourcecode--Online Book Store	A vulnerability, which was classified as critical, was found in itsourcecode Online Book Store up to 1.0. Affected is an unknown function of the file /edit_book.php. The manipulation of the argument image 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-268698 is the identifier assigned to this vulnerability.	2024-06-15	6.3	CVE-2024-6008

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
itsourcecode--Online Book Store	A vulnerability was found in itsourcecode Online Book Store 1.0. It has been rated as critical. This issue affects some unknown processing of the file admin_delete.php. The manipulation of the argument bookisbn leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-268721 was assigned to this vulnerability.	2024-06-15	6.3	CVE-2024-6013
itsourcecode--Online House Rental System	A vulnerability was found in itsourcecode Online House Rental System 1.0. It has been classified as critical. Affected is an unknown function of the file manage_user.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-268458 is the identifier assigned to this vulnerability.	2024-06-14	6.3	CVE-2024-5981
itsourcecode--Online House Rental System	A vulnerability classified as critical was found in itsourcecode Online House Rental System 1.0. Affected by this vulnerability is an unknown functionality of the file manage_user.php. The manipulation of the argument month_of 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-268723.	2024-06-15	6.3	CVE-2024-6015
itsourcecode--Online Laundry Management System	A vulnerability, which was classified as critical, has been found in itsourcecode Online Laundry Management System 1.0. Affected by this issue is some unknown functionality of the file admin_class.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-268724.	2024-06-15	6.3	CVE-2024-6016
itsourcecode--Payroll Management System	A vulnerability was found in itsourcecode Payroll Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file print_payroll.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-268142 is the identifier assigned to this vulnerability.	2024-06-12	6.3	CVE-2024-5898
jasonraimondi--url-to-png	@jmondi/url-to-png is a self-hosted URL to PNG utility. Versions prior to 2.0.3 are vulnerable to arbitrary file read if a threat actor uses the Playright's screenshot feature to exploit the file wrapper. Version 2.0.3 mitigates this issue by requiring input URLs to be of protocol `http` or `https`. No known workarounds are available aside from upgrading.	2024-06-10	5.3	CVE-2024-37169
jegtheme--Jeg Elementor Kit	The Jeg Elementor Kit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the sg_general_toggle_tab_enable and sg_accordion_style attributes within the plugin's JKit - Tabs and JKit - Accordion widget, respectively, in all versions up to, and including, 2.6.5 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.	2024-06-15	6.4	CVE-2024-4479
jetmonsters--Stratum Elementor Widgets	The Stratum - Elementor Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'label_years' attribute within the Countdown widget in all versions up to, and including, 1.4.1 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.	2024-06-15	6.4	CVE-2024-5611
ladela--WordPress Online Booking and Scheduling Plugin Bookly	The WordPress Online Booking and Scheduling Plugin - Bookly plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Color Profile parameter in all versions up to, and including, 23.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with the staff member role and Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-11	6.4	CVE-2024-5584

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
leap13--Premium Addons for Elementor	The Premium Addons for Elementor plugin for WordPress is vulnerable to DOM-Based Stored Cross-Site Scripting via several parameters in all versions up to, and including, 4.10.33 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 and edits an injected element, and subsequently clicks the element with the mouse scroll wheel.	2024-06-12	4.4	CVE-2024-5553
Lim Kai Yang--Grab & Save	Cross-Site Request Forgery (CSRF) vulnerability in Lim Kai Yang Grab & Save.This issue affects Grab & Save: from n/a through 1.0.4.	2024-06-12	4.3	CVE-2023-47845
LINE Corporation--LINE client for iOS	The in-app browser of LINE client for iOS versions below 14.9.0 contains a Universal XSS (UXSS) vulnerability. This vulnerability allows for cross-site scripting (XSS) where arbitrary JavaScript can be executed in the top frame from an embedded iframe on any displayed web site within the in-app browser. The in-app browser is usually opened by tapping on URLs contained in chat messages, and for the attack to be successful, the victim must trigger a click event on a malicious iframe. If an iframe embedded in any website can be controlled by an attacker, this vulnerability could be exploited to capture or alter content displayed in the top frame, as well as user session information. This vulnerability affects LINE client for iOS versions below 14.9.0 and does not affect other LINE clients such as LINE client for Android. Please update LINE client for iOS to version 14.9.0 or higher.	2024-06-12	6.1	CVE-2024-5739 dl_cve@linecorp.com
MailerLite--MailerLite WooCommerce integration	Missing Authorization vulnerability in MailerLite MailerLite - WooCommerce integration.This issue affects MailerLite - WooCommerce integration: from n/a through 2.0.8.	2024-06-11	4.3	CVE-2023-52227
Mandrill--wpMandrill	Missing Authorization vulnerability in Mandrill wpMandrill.This issue affects wpMandrill: from n/a through 1.33.	2024-06-12	4.3	CVE-2023-47828
Mattermost--Mattermost	Mattermost Desktop App versions <=5.7.0 fail to correctly prompt for permission when opening external URLs which allowsÂ a remote attacker to force a victim over the Internet to run arbitrary programs on the victim's systemÂ via custom URI schemes.	2024-06-14	4.7	CVE-2024-37182
Matthias Pfefferle & Automattic--ActivityPub	Missing Authorization vulnerability in Matthias Pfefferle & Automattic ActivityPub.This issue affects ActivityPub: from n/a through 1.0.5.	2024-06-11	6.5	CVE-2023-52199
Maxime Schoeni--Sublanguage	Missing Authorization vulnerability in Maxime Schoeni Sublanguage.This issue affects Sublanguage: from n/a through 2.9.	2024-06-14	5.4	CVE-2023-36695
meowapps --database_cleaner	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Jordy Meow Database Cleaner allows Relative Path Traversal.This issue affects Database Cleaner: from n/a through 1.0.5.	2024-06-10	4.9	CVE-2024-35712
Metagauss--ProfileGrid	Missing Authorization vulnerability in Metagauss ProfileGrid.This issue affects ProfileGrid: from n/a through 5.6.6.	2024-06-12	4.3	CVE-2023-52117
metersphere--metersphere	MeterSphere is an open source continuous testing platform. Prior to version 1.10.1-lts, the system's step editor stores cross-site scripting vulnerabilities. Version 1.10.1-lts fixes this issue.	2024-06-11	4	CVE-2024-37161

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mgibbs189--Custom Field Suite	The Custom Field Suite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the the 'cfs[post_content]' parameter versions up to, and including, 2.6.7 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.	2024-06-12	6.4	CVE-2024-3559
Microsoft--Azure File Sync	Microsoft Azure File Sync Elevation of Privilege Vulnerability	2024-06-11	4.4	CVE-2024-35253
Microsoft--Azure Identity Library for .NET	Azure Identity Libraries and Microsoft Authentication Library Elevation of Privilege Vulnerability	2024-06-11	5.5	CVE-2024-35255
Microsoft--Microsoft Dynamics 365 (on-premises) version 9.1	Microsoft Dynamics 365 (On-Premises) Information Disclosure Vulnerability	2024-06-11	5.7	CVE-2024-35263
Microsoft--Microsoft Edge (Chromium-based)	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-06-13	5.4	CVE-2024-30058
Microsoft--Microsoft Edge for iOS	Microsoft Edge for iOS Spoofing Vulnerability	2024-06-13	5.4	CVE-2024-30057
Microsoft--Microsoft Edge for iOS	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-06-13	4.3	CVE-2024-38083
Microsoft--Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)	Visual Studio Remote Code Execution Vulnerability	2024-06-11	4.7	CVE-2024-30052
Microsoft--Microsoft Visual Studio 2022 version 17.10	Visual Studio Elevation of Privilege Vulnerability	2024-06-11	6.7	CVE-2024-29060
Microsoft--Windows 10 Version 1809	Windows Distributed File System (DFS) Remote Code Execution Vulnerability	2024-06-11	6.7	CVE-2024-30063
Microsoft--Windows 10 Version 1809	Windows Container Manager Service Elevation of Privilege Vulnerability	2024-06-11	6.8	CVE-2024-30076

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows 10 Version 1809	Windows Themes Denial of Service Vulnerability	2024-06-11	5.5	CVE-2024-30065
Microsoft--Windows 10 Version 1809	Winlogon Elevation of Privilege Vulnerability	2024-06-11	5.5	CVE-2024-30066
Microsoft--Windows 10 Version 1809	Winlogon Elevation of Privilege Vulnerability	2024-06-11	5.5	CVE-2024-30067
Microsoft--Windows 10 Version 1809	Windows Cryptographic Services Information Disclosure Vulnerability	2024-06-11	5.5	CVE-2024-30096
Microsoft--Windows 10 Version 1809	Windows Remote Access Connection Manager Information Disclosure Vulnerability	2024-06-11	4.7	CVE-2024-30069
Minoji--MJ Update History	Missing Authorization vulnerability in Minoji MJ Update History.This issue affects MJ Update History: from n/a through 1.0.4.	2024-06-11	4.3	CVE-2024-35671
mlewand--ckeditor-plugin-openlink	The Open Link is a CKEditor plugin, extending context menu with a possibility to open link in a new tab. The vulnerability allowed to execute JavaScript code by abusing link href attribute. It affects all users using the Open Link plugin at version < **1.0.5**.	2024-06-14	6.1	CVE-2024-37888
MoreConvert--MC Woocommerce Wishlist	Missing Authorization vulnerability in MoreConvert MC Woocommerce Wishlist.This issue affects MC Woocommerce Wishlist: from n/a through 1.7.8.	2024-06-11	5.3	CVE-2024-34813
MoreConvert--MC Woocommerce Wishlist	Missing Authorization vulnerability in MoreConvert MC Woocommerce Wishlist.This issue affects MC Woocommerce Wishlist: from n/a through 1.7.2.	2024-06-11	5.3	CVE-2024-34819
n/a--n/a	A Directory Traversal vulnerability in iceice666 ResourcePack Server before v1.0.8 allows a remote attacker to disclose files on the server, via setPath in ResourcePackFileServer.kt.	2024-06-10	6.5	CVE-2024-35474
n/a--Newspaper - News & WooCommerce WordPress Theme	The Newspaper theme for WordPress is vulnerable to Stored Cross-Site Scripting via attachment meta in the archive page in all versions up to, and including, 12.6.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-15	5.5	CVE-2024-3815
N/A--Piotnet Forms	Missing Authorization vulnerability in Piotnet Forms.This issue affects Piotnet Forms: from n/a through 1.0.29.	2024-06-12	5.3	CVE-2023-51413
namithjawahar--Insert Post Ads	Missing Authorization vulnerability in namithjawahar Insert Post Ads.This issue affects Insert Post Ads: from n/a through 1.3.2.	2024-06-11	5.3	CVE-2024-35665

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Navneil Naicker--ACF Photo Gallery Field	Missing Authorization vulnerability in Navneil Naicker ACF Photo Gallery Field.This issue affects ACF Photo Gallery Field: from n/a through 2.6.	2024-06-11	4.3	CVE-2024-23518
NervyThemes--SKU Label Changer For WooCommerce	Missing Authorization vulnerability in NervyThemes SKU Label Changer For WooCommerce.This issue affects SKU Label Changer For WooCommerce: from n/a through 3.0.	2024-06-14	6.5	CVE-2023-29174
NetApp--StorageGRID (formerly StorageGRID Webscale)	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.7.0.9 and 11.8.0.5 are susceptible to disclosure of sensitive information via complex MiTM attacks due to a vulnerability in the SSH cryptographic implementation.	2024-06-14	5.3	CVE-2024-21988 security-alert@netapp.com
Netentsec--NS-ASG Application Security Gateway	A vulnerability classified as critical has been found in Netentsec NS-ASG Application Security Gateway 6.3. This affects an unknown part of the file /protocol/iscgwtunnel/deleteiscgwrouteconf.php. The manipulation of the argument messagecontent leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-268695. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-15	6.3	CVE-2024-6007
netgsm -- netgsm	Missing Authorization vulnerability in Netgsm.This issue affects Netgsm: from n/a through 2.9.16.	2024-06-10	6.3	CVE-2024-4746
netweblogic--Events Manager Calendar, Bookings, Tickets, and more!	The Events Manager - Calendar, Bookings, Tickets, and more! plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'event', 'location', and 'event_category' shortcodes in all versions up to, and including, 6.4.7.3 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.	2024-06-12	6.4	CVE-2024-3492
nextcloud--security-advisories	user_oidc app is an OpenID Connect user backend for Nextcloud. Missing access control on the ID4me endpoint allows an attacker to register an account eventually getting access to data that is available to all registered users. It is recommended that the OpenID Connect user backend is upgraded to 3.0.0 (Nextcloud 20-23), 4.0.0 (Nexcloud 24) or 5.0.0 (Nextcloud 25-28).	2024-06-14	6.3	CVE-2024-37312
nextcloud--security-advisories	user_oidc app is an OpenID Connect user backend for Nextcloud. An attacker could potentially trick the app into accepting a request that is not signed by the correct server. It is recommended that the Nextcloud user_oidc app is upgraded to 1.3.5, 2.0.0, 3.0.0, 4.0.0 or 5.0.0.	2024-06-14	5.4	CVE-2024-37886
nextcloud--security-advisories	Nextcloud Calendar is a calendar app for Nextcloud. Authenticated users could create an event with manipulated attachment data leading to a bad redirect for participants when clicked. It is recommended that the Nextcloud Calendar App is upgraded to 4.6.8 or 4.7.2.	2024-06-14	4.6	CVE-2024-37316
nextcloud--security-advisories	The Nextcloud Notes app is a distraction free notes taking app for Nextcloud. If an attacker managed to share a folder called `Notes/` with a newly created user before they logged in, the Notes app would use that folder store the personal notes. It is recommended that the Nextcloud Notes app is upgraded to 4.9.3.	2024-06-14	4.6	CVE-2024-37317
nextcloud--security-advisories	Nextcloud Deck is a kanban style organization tool aimed at personal planning and project organization for teams integrated with Nextcloud. A user with access to a deck board was able to access comments and attachments of already deleted	2024-06-14	4.3	CVE-2024-37883

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	cards. It is recommended that the Nextcloud Deck app is upgraded to 1.6.6 or 1.7.5 or 1.8.7 or 1.9.6 or 1.11.3 or 1.12.1.			
nicheaddons--Events Addon for Elementor	The Events Addon for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Basic Slider, Upcoming Events, and Schedule widgets in all versions up to, and including, 2.1.4 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.	2024-06-11	6.4	CVE-2024-4669
NuGet--NuGetGallery	NuGet Gallery is a package repository that powers nuget.org. The NuGetGallery has a security vulnerability related to its handling of autolinks in Markdown content. While the platform properly filters out JavaScript from standard links, it does not adequately sanitize autolinks. This oversight allows attackers to exploit autolinks as a vector for Cross-Site Scripting (XSS) attacks. When a user inputs a Markdown autolink such as `<javascript:alert(1)>`, the link is rendered without proper sanitization. This means that the JavaScript code within the autolink can be executed by the browser, leading to an XSS attack. Version 2024.05.28 contains a patch for this issue.	2024-06-12	6.1	CVE-2024-37304
nvidia--GPU display driver, vGPU software, and Cloud Gaming	NVIDIA GPU Driver for Windows and Linux contains a vulnerability where an improper check or improper handling of exception conditions might lead to denial of service.	2024-06-13	5.5	CVE-2024-0092
nvidia--NVIDIA Triton Inference Server	NVIDIA Triton Inference Server for Linux contains a vulnerability where a user may cause an incorrect Initialization of resource by network issue. A successful exploit of this vulnerability may lead to information disclosure.	2024-06-13	5.4	CVE-2024-0103
nvidia--vGPU software and Cloud Gaming	NVIDIA vGPU software for Windows and Linux contains a vulnerability where unprivileged users could execute privileged operations on the host. A successful exploit of this vulnerability might lead to data tampering, escalation of privileges, and denial of service.	2024-06-13	6.3	CVE-2024-0085
nvidia--vGPU software and Cloud Gaming	NVIDIA GPU software for Linux contains a vulnerability where it can expose sensitive information to an actor that is not explicitly authorized to have access to that information. A successful exploit of this vulnerability might lead to information disclosure.	2024-06-13	6.5	CVE-2024-0093
nvidia--vGPU software and Cloud Gaming	NVIDIA vGPU software for Linux contains a vulnerability where the software can dereference a NULL pointer. A successful exploit of this vulnerability might lead to denial of service and undefined behavior in the vGPU plugin.	2024-06-13	5.5	CVE-2024-0086
nvidia--vGPU software and Cloud Gaming	NVIDIA vGPU software for Linux contains a vulnerability in the Virtual GPU Manager, where an untrusted guest VM can cause improper control of the interaction frequency in the host. A successful exploit of this vulnerability might lead to denial of service.	2024-06-13	5.5	CVE-2024-0094
oceanwp--Ocean Extra	The Ocean Extra plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Flickr widget in all versions up to, and including, 2.2.8 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.	2024-06-11	6.4	CVE-2024-5531

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ONTRAPORT Inc.--PilotPress	Missing Authorization vulnerability in ONTRAPORT Inc. PilotPress.This issue affects PilotPress: from n/a through 2.0.30.	2024-06-10	5.3	CVE-2024-23524
open-quantum-safe--liboqs	liboqs is a C-language cryptographic library that provides implementations of post-quantum cryptography algorithms. A control-flow timing lean has been identified in the reference implementation of the Kyber key encapsulation mechanism when it is compiled with Clang 15-18 for `-Os`, `-O1`, and other compilation options. A proof-of-concept local attack on the reference implementation leaks the entire ML-KEM 512 secret key in ~10 minutes using end-to-end decapsulation timing measurements. The issue has been fixed in version 0.10.1. As a possible workaround, some compiler options may produce vectorized code that does not leak secret information, however relying on these compiler options as a workaround may not be reliable.	2024-06-10	5.9	CVE-2024-36405
OpenPrinting--cups	OpenPrinting CUPS is an open source printing system for Linux and other Unix-like operating systems. In versions 2.4.8 and earlier, when starting the cupsd server with a Listen configuration item pointing to a symbolic link, the cupsd process can be caused to perform an arbitrary chmod of the provided argument, providing world-writable access to the target. Given that cupsd is often running as root, this can result in the change of permission of any user or system files to be world writable. Given the aforementioned Ubuntu AppArmor context, on such systems this vulnerability is limited to those files modifiable by the cupsd process. In that specific case it was found to be possible to turn the configuration of the Listen argument into full control over the cupsd.conf and cups-files.conf configuration files. By later setting the User and Group arguments in cups-files.conf, and printing with a printer configured by PPD with a `FoomaticRIPCommandLine` argument, arbitrary user and group (not root) command execution could be achieved, which can further be used on Ubuntu systems to achieve full root command execution. Commit ff1f8a623e090dee8a8aadf12a6a4b25efac143d contains a patch for the issue.	2024-06-11	4.4	CVE-2024-35235
OpenText--NetIQ Access Manager	This allows the information exposure to unauthorized users.Â This issue affects NetIQ Access Manager using version 4.5 or before	2024-06-11	6.5	CVE-2020-11843
ovic_importer_project --ovic_importer	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Ovic Team Ovic Importer allows Path Traversal.This issue affects Ovic Importer: from n/a through 1.6.3.	2024-06-10	6.5	CVE-2024-35754
Photo Gallery Team--Photo Gallery by 10Web	Missing Authorization vulnerability in Photo Gallery Team Photo Gallery by 10Web.This issue affects Photo Gallery by 10Web: from n/a through 1.8.24.	2024-06-11	4.3	CVE-2024-35628
Podlove--Podlove Podcast Publisher	Missing Authorization vulnerability in Podlove Podlove Podcast Publisher.This issue affects Podlove Podcast Publisher: from n/a through 4.1.0.	2024-06-11	4.3	CVE-2024-32143
quantumcloud--AI Infographic Maker	The AI Infographic Maker plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the qcld_openai_title_generate_desc AJAX action in all versions up to, and including, 4.7.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update arbitrary post titles.	2024-06-15	4.3	CVE-2024-5858
RabbitLoader--RabbitLoader	Missing Authorization vulnerability in RabbitLoader.This issue affects RabbitLoader: from n/a through 2.19.13.	2024-06-10	5.4	CVE-2024-21751

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--Red Hat Enterprise Linux 6	A vulnerability was found in GNU Nano that allows a possible privilege escalation through an insecure temporary file. If Nano is killed while editing, a file it saves to an emergency file with the permissions of the running user provides a window of opportunity for attackers to escalate privileges through a malicious symlink.	2024-06-12	4.7	CVE-2024-5742
Red Hat--Red Hat Quay 3	A vulnerability was found in Quay. If an attacker can obtain the client ID for an application, they can use an OAuth token to authenticate despite not having access to the organization from which the application was created. This issue is limited to authentication and not authorization. However, in configurations where endpoints rely only on authentication, a user may authenticate to applications they otherwise have no access to.	2024-06-12	4.2	CVE-2024-5891
Repute Infosystems--BookingPress	Missing Authorization vulnerability in Repute Infosystems BookingPress.This issue affects BookingPress: from n/a through 1.0.82.	2024-06-11	6.5	CVE-2024-34799
Revolut--Revolut Gateway for WooCommerce	Missing Authorization vulnerability in Revolut Revolut Gateway for WooCommerce.This issue affects Revolut Gateway for WooCommerce: from n/a through 4.9.7.	2024-06-11	4.3	CVE-2023-52224
salesagility -- suitecrm	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, a user password can be reset from an unauthenticated attacker. The attacker does not get access to the new password. But this can be annoying for the user. This attack is also dependent on some password reset functionalities being enabled. It also requires the system using php 7, which is not an officially supported version. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	2024-06-10	6.5	CVE-2024-36407
salesagility -- suitecrm	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in the connectors file verification allows for a server-side request forgery attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	2024-06-10	6.5	CVE-2024-36414
salesagility -- suitecrm	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in the import module error view allows for a cross-site scripting attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	2024-06-10	5.4	CVE-2024-36413
salesagility--SuiteCRM	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, unchecked input allows for open re-direct. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	2024-06-10	5.4	CVE-2024-36406
salesagility--SuiteCRM-Core	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. A vulnerability in versions prior to 8.6.1 allows for Host Header Injection when directly accessing the `/legacy` route. Version 8.6.1 contains a patch for the issue.	2024-06-10	4.3	CVE-2024-36419
Salesforce--Pardot	Missing Authorization vulnerability in Salesforce Pardot.This issue affects Pardot: from n/a through 2.1.0.	2024-06-11	4.3	CVE-2024-32148
SAP_SE--SAP BW/4HANA Transformation and Data Transfer Process	SAP BW/4HANA Transformation and Data Transfer Process (DTP) allows an authenticated attacker to gain higher access levels than they should have by exploiting improper authorization checks. This results in escalation of privileges. It has no impact on the confidentiality of data but may have low impacts on the integrity and availability of the application.	2024-06-11	5.5	CVE-2024-37176
SAP_SE--SAP CRM WebClient UI	Due to insufficient input validation, SAP CRM WebClient UI allows an unauthenticated attacker to craft a URL link which embeds a malicious script. When a victim clicks on this link, the script will be executed in the victim's browser	2024-06-11	6.1	CVE-2024-34686

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	giving the attacker the ability to access and/or modify information with no effect on availability of the application.			
SAP_SE--SAP Document Builder	An authenticated attacker can upload malicious file to SAP Document Builder service. When the victim accesses this file, the attacker is allowed to access, modify, or make the related information unavailable in the victim's browser.	2024-06-11	6.5	CVE-2024-34683
SAP_SE--SAP Financial Consolidation	SAP Financial Consolidation does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. These endpoints are exposed over the network. The vulnerability can exploit resources beyond the vulnerable component. On successful exploitation, an attacker can cause limited impact to confidentiality of the application.	2024-06-11	5	CVE-2024-37178
SAP_SE--SAP NetWeaver and ABAP platform	SAP NetWeaver and ABAP platform allows an attacker to impede performance for legitimate users by crashing or flooding the service. An impact of this Denial of Service vulnerability might be long response delays and service interruptions, thus degrading the service quality experienced by legitimate users causing high impact on availability of the application.	2024-06-11	6.5	CVE-2024-33001
SAP_SE--SAP NetWeaver AS Java	SAP NetWeaver AS Java (CAF - Guided Procedures) allows an unauthenticated user to access non-sensitive information about the server which would otherwise be restricted causing low impact on confidentiality of the application.	2024-06-11	5.3	CVE-2024-28164
SAP_SE--SAP S/4HANA (Manage Incoming Payment Files)	Manage Incoming Payment Files (F1680) of SAP S/4HANA does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. As a result, it has high impact on integrity and no impact on the confidentiality and availability of the system.	2024-06-11	6.5	CVE-2024-34691
SAP_SE--SAP Student Life Cycle Management	SAP Student Life Cycle Management (SLcM) fails to conduct proper authorization checks for authenticated users, leading to the potential escalation of privileges. On successful exploitation it could allow an attacker to access and edit non-sensitive report variants that are typically restricted, causing minimal impact on the confidentiality and integrity of the application.	2024-06-11	5.4	CVE-2024-34690
sc_filechecker_project -- sc_filechecker	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Siteclean SC filechecker allows Path Traversal, File Manipulation.This issue affects SC filechecker: from n/a through 0.6.	2024-06-10	6.5	CVE-2024-35743
Schneider Electric--EVlink Home Smart	CWE-668: Exposure of the Resource Wrong Sphere vulnerability exists that exposes a SSH interface over the product network interface. This does not allow to directly exploit the product or make any unintended operation as the SSH interface access is protected by an authentication mechanism. Impacts are limited to port scanning and fingerprinting activities as well as attempts to perform a potential denial of service attack on the exposed SSH interface.	2024-06-12	6.5	CVE-2024-5313
Schneider Electric--Modicon M340	CWE-552: Files or Directories Accessible to External Parties vulnerability exists which may prevent user to update the device firmware and prevent proper behavior of the webserver when specific files or directories are removed from the filesystem.	2024-06-12	6.5	CVE-2024-5056
Schneider Electric--PowerLogic P5	CWE-327: Use of a Broken or Risky Cryptographic Algorithm vulnerability exists that could cause denial of service, device reboot, or an attacker gaining full control of the relay when a specially crafted reset token is entered into the front panel of the device.	2024-06-12	6.1	CVE-2024-5559
Schneider Electric--Sage 1410	CWE-252: Unchecked Return Value vulnerability exists that could cause denial of service of the device when an attacker sends a specially crafted HTTP request.	2024-06-12	5.9	CVE-2024-37039

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Schneider Electric--Sage 1410	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability exists that could allow a user with access to the device's web interface to cause a fault on the device when sending a malformed HTTP request.	2024-06-12	5.4	CVE-2024-37040
Schneider Electric--Sage 1410	CWE-125: Out-of-bounds Read vulnerability exists that could cause denial of service of the device's web interface when an attacker sends a specially crafted HTTP request.	2024-06-12	5.3	CVE-2024-5560
Schneider Electric--SpaceLogic AS-P	CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability exists that could cause escalation of privileges when an attacker abuses a limited admin account.	2024-06-12	6.4	CVE-2024-5558
Schneider Electric--SpaceLogic AS-P	CWE-532: Insertion of Sensitive Information into Log File vulnerability exists that could cause exposure of SNMP credentials when an attacker has access to the controller logs.	2024-06-12	4.5	CVE-2024-5557
seedprod -- rafflepress	Missing Authorization vulnerability in RafflePress Giveaways and Contests by RafflePress.This issue affects Giveaways and Contests by RafflePress: from n/a through 1.12.4.	2024-06-10	6.3	CVE-2024-4745
SendPress--SendPress Newsletters	Missing Authorization vulnerability in SendPress SendPress Newsletters.This issue affects SendPress Newsletters: from n/a through 1.23.11.6.	2024-06-14	5.3	CVE-2023-35040
Siemens--Mendix Applications using Mendix 10	A vulnerability has been identified in Mendix Applications using Mendix 10 (All versions < V10.11.0), Mendix Applications using Mendix 10 (V10.6) (All versions < V10.6.9), Mendix Applications using Mendix 9 (All versions >= V9.3.0 < V9.24.22). Affected applications could allow users with the capability to manage a role to elevate the access rights of users with that role. Successful exploitation requires to guess the id of a target role which contains the elevated access rights.	2024-06-11	5.9	CVE-2024-33500
Siemens--SIMATIC CP 1542SP-1	A vulnerability has been identified in SIMATIC CP 1542SP-1 (6GK7542-6UX00-0XE0) (All versions < V2.3), SIMATIC CP 1542SP-1 IRC (6GK7542-6VX00-0XE0) (All versions < V2.3), SIMATIC CP 1543SP-1 (6GK7543-6WX00-0XE0) (All versions < V2.3), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (6AG2542-6VX00-4XE0) (All versions < V2.3), SIPLUS ET 200SP CP 1543SP-1 ISEC (6AG1543-6WX00-7XE0) (All versions < V2.3), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (6AG2543-6WX00-4XE0) (All versions < V2.3), SIPLUS TIM 1531 IRC (6AG1543-1MX00-7XE0) (All versions < V2.4.8), TIM 1531 IRC (6GK7543-1MX00-0XE0) (All versions < V2.4.8). The web server of affected products, if configured to allow the import of PKCS12 containers, could end up in an infinite loop when processing incomplete certificate chains. This could allow an authenticated remote attacker to create a denial of service condition by importing specially crafted PKCS12 containers.	2024-06-11	4.9	CVE-2023-50763
Siemens--SINEC Traffic Analyzer	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V1.2). The affected web server stored the password in cleartext. This could allow attacker in a privileged position to obtain access passwords.	2024-06-11	6.3	CVE-2024-35208
Siemens--SINEC Traffic Analyzer	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V1.2). The affected web server is not enforcing HSTS. This could allow an attacker to perform downgrade attacks exposing confidential information.	2024-06-11	6.5	CVE-2024-35210
Siemens--SINEC Traffic Analyzer	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V1.2). The affected web server, after a successful login, sets the session cookie on the browser, without applying any security attributes (such as "Secure", "HttpOnly", or "SameSite").	2024-06-11	6.5	CVE-2024-35211

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SoftLab--Integrate Google Drive	Missing Authorization vulnerability in SoftLab Integrate Google Drive.This issue affects Integrate Google Drive: from n/a through 1.3.3.	2024-06-12	5.4	CVE-2023-52177
SoftLab--Radio Player	Missing Authorization vulnerability in SoftLab Radio Player.This issue affects Radio Player: from n/a through 2.0.73.	2024-06-11	5.3	CVE-2024-34753
Soliloquy Team--Slider by Soliloquy	Missing Authorization vulnerability in Soliloquy Team Slider by Soliloquy.This issue affects Slider by Soliloquy: from n/a through 2.7.2.	2024-06-11	4.3	CVE-2023-51519
SourceCodester--Best Online News Portal	A vulnerability classified as critical has been found in SourceCodester Best Online News Portal 1.0. This affects an unknown part of the file /admin/index.php. The manipulation of the argument username 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-268461 was assigned to this vulnerability.	2024-06-14	6.3	CVE-2024-5985
SourceCodester--Cab Management System	A vulnerability classified as critical has been found in SourceCodester Cab Management System 1.0. This affects an unknown part of the file /cms/classes/Users.php?f=delete_client. 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-268137 was assigned to this vulnerability.	2024-06-12	6.3	CVE-2024-5893
SourceCodester--Employee and Visitor Gate Pass Logging System	A vulnerability, which was classified as critical, has been found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. This issue affects the function delete_users of the file /classes/Users.php?f=delete. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-268139.	2024-06-12	6.3	CVE-2024-5895
SourceCodester--Employee and Visitor Gate Pass Logging System	A vulnerability has been found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /classes/Master.php?f=log_visitor. The manipulation of the argument name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-268141 was assigned to this vulnerability.	2024-06-12	4.3	CVE-2024-5897
specialk--Dashboard Widgets Suite	The Dashboard Widgets Suite plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in all versions up to, and including, 3.4.3 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.	2024-06-13	6.1	CVE-2024-0979
strapi--strapi	Strapi is an open-source content management system. Prior to version 4.22.0, a denial-of-service vulnerability is present in the media upload process causing the server to crash without restarting, affecting either development and production environments. Usually, errors in the application cause it to log the error and keep it running for other clients. This behavior, in contrast, stops the server execution, making it unavailable for any clients until it's manually restarted. Any user with access to the file upload functionality is able to exploit this vulnerability, affecting applications running in both development mode and production mode as well. Users should upgrade @strapi/plugin-upload to version 4.22.0 to receive a patch.	2024-06-12	5.3	CVE-2024-31217
stylemix--WordPress Header Builder Plugin Pearl	The WordPress Header Builder Plugin - Pearl plugin for WordPress is vulnerable to unauthorized site option deletion due to a missing validation and capability checks on the stm_hb_delete() function in all versions up to, and including, 1.3.7. This makes it possible for unauthenticated attackers to delete arbitrary options that can be used to perform a denial of service attack on a site.	2024-06-12	6.5	CVE-2024-5468

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tabrisrp--WPS Hide Login	The WPS Hide Login plugin for WordPress is vulnerable to Login Page Disclosure in all versions up to, and including, 1.9.15.2. This is due to a bypass that is created when the 'action=postpass' parameter is supplied. This makes it possible for attackers to easily discover any login page that may have been hidden by the plugin.	2024-06-11	5.3	CVE-2024-2473
tagDiv--tagDiv Composer	The tagDiv Composer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'single' module in all versions up to, and including, 4.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-15	5.5	CVE-2024-3814
Tagembed--Tagembed	Missing Authorization vulnerability in Tagembed.This issue affects Tagembed: from n/a through 5.5.	2024-06-11	5.4	CVE-2024-34804
TechnoVama--Quotes for WooCommerce	Missing Authorization vulnerability in TechnoVama Quotes for WooCommerce.This issue affects Quotes for WooCommerce: from n/a through 2.0.1.	2024-06-12	4.3	CVE-2023-51680
Tenable--Security Center	An improper privilege management vulnerability exists in Tenable Security Center where an authenticated, remote attacker could view unauthorized objects and launch scans without having the required privileges	2024-06-12	5.4	CVE-2024-5759 vulnreport@tenable.com
Teplitsa of social technologies--Leyka	Missing Authorization vulnerability in Teplitsa of social technologies Leyka.This issue affects Leyka: from n/a through 3.31.1.	2024-06-11	5.3	CVE-2024-35683
Termly--Cookie Consent	Missing Authorization vulnerability in Termly Cookie Consent.This issue affects Cookie Consent: from n/a through 3.2.	2024-06-11	5.3	CVE-2024-35692
The Newsletter Team--Newsletter - API v1 and v2 addon for Newsletter	The Newsletter - API v1 and v2 addon plugin for WordPress is vulnerable to unauthorized subscribers management due to PHP type juggling issue on the check_api_key function in all versions up to, and including, 2.4.5. This makes it possible for unauthenticated attackers to list, create or delete newsletter subscribers. This issue affects only sites running the PHP version below 8.0	2024-06-12	6.5	CVE-2024-5674
ThemeBoy--SportsPress Sports Club & League Manager	Missing Authorization vulnerability in ThemeBoy SportsPress - Sports Club & League Manager.This issue affects SportsPress - Sports Club & League Manager: from n/a through 2.7.20.	2024-06-11	4.3	CVE-2024-34824
themeisle --product_addons_\&_fields_for_woocommerce	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in Themeisle PPOM for WooCommerce allows Code Inclusion.This issue affects PPOM for WooCommerce: from n/a through 32.0.20.	2024-06-10	5.3	CVE-2024-35728
TMS--Amelia	Missing Authorization vulnerability in TMS Amelia ameliabooking.This issue affects Amelia: from n/a through 1.0.98.	2024-06-10	5.3	CVE-2024-22298
Tobias Conrad--Builder for WooCommerce reviews shortcodes	Missing Authorization vulnerability in Tobias Conrad Builder for WooCommerce reviews shortcodes - ReviewShort.This issue affects Builder for WooCommerce reviews shortcodes - ReviewShort: from n/a through 1.01.5.	2024-06-11	5.3	CVE-2024-34763

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ReviewShort				
Tobias Conrad--Design for Contact Form 7 Style WordPress Plugin CF7 WOW Styler	Missing Authorization vulnerability in Tobias Conrad Design for Contact Form 7 Style WordPress Plugin - CF7 WOW Styler.This issue affects Design for Contact Form 7 Style WordPress Plugin - CF7 WOW Styler: from n/a through 1.6.4.	2024-06-11	6.3	CVE-2024-34826
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	The Toshiba printers do not implement privileges separation. As for the affected products/models/versions, see the reference URL.	2024-06-14	6.7	CVE-2024-27146
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	Passwords are stored in clear-text logs. An attacker can retrieve passwords. As for the affected products/models/versions, see the reference URL.	2024-06-14	6.2	CVE-2024-27154
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	The session cookies, used for authentication, are stored in clear-text logs. An attacker can retrieve authentication sessions. A remote attacker can retrieve the credentials and bypass the authentication mechanism. As for the affected products/models/versions, see the reference URL.	2024-06-14	6.8	CVE-2024-27156
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	The sessions are stored in clear-text logs. An attacker can retrieve authentication sessions. A remote attacker can retrieve the credentials and bypass the authentication mechanism. As for the affected products/models/versions, see the reference URL.	2024-06-14	6.8	CVE-2024-27157
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	All the Toshiba printers contain a shell script using the same hardcoded key to encrypt logs. An attacker can decrypt the encrypted files using the hardcoded key. This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone. So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability. For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	2024-06-14	6.2	CVE-2024-27159
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	All the Toshiba printers contain a shell script using the same hardcoded key to encrypt logs. An attacker can decrypt the encrypted files using the hardcoded key. This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone. So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability. For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	2024-06-14	6.2	CVE-2024-27160

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	all the Toshiba printers have programs containing a hardcoded key used to encrypt files. An attacker can decrypt the encrypted files using the hardcoded key. Insecure algorithm is used for the encryption. This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone. So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability.Â For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	2024-06-14	6.2	CVE-2024-27161
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	Toshiba printers provide a web interface that will load the JavaScript file. The file contains insecure codes vulnerable to XSS and is loaded inside all the webpages provided by the printer. An attacker can steal the cookie of an admin user. As for the affected products/models/versions, see the reference URL.	2024-06-14	6.1	CVE-2024-27162
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	Toshiba printers will display the password of the admin user in clear-text and additional passwords when sending 2 specific HTTP requests to the internal API. An attacker stealing the cookie of an admin or abusing a XSS vulnerability can recover this password in clear-text and compromise the printer. This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone. So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability. For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	2024-06-14	6.5	CVE-2024-27163
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	An attacker with admin access can install rogue applications. As for the affected products/models/versions, see the reference URL.	2024-06-14	6.7	CVE-2024-27180
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	Toshiba printers use XML communication for the API endpoint provided by the printer. For the endpoint, XML parsing library is used and it is vulnerable to a time-based blind XML External Entity (XXE) vulnerability. An attacker can DoS the printers by sending a HTTP request without authentication. An attacker can exploit the XXE to retrieve information.Â As for the affected products/models/versions, see the reference URL.	2024-06-14	5.9	CVE-2024-27141
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	Toshiba printers use XML communication for the API endpoint provided by the printer. For the endpoint, XML parsing library is used and it is vulnerable to a time-based blind XML External Entity (XXE) vulnerability. An attacker can DoS the printers. An attacker can exploit the XXE to retrieve information. As for the affected products/models/versions, see the reference URL.	2024-06-14	5.9	CVE-2024-27142
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	Remote Command program allows an attacker to read any file using a Local File Inclusion vulnerability. An attacker can read any file on the printer. As for the affected products/models/versions, see the reference URL.	2024-06-14	4.4	CVE-2024-27175

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Toshiba Tec Corporation--Toshiba Tec e-Studio multi-function peripheral (MFP)	Admin cookies are written in clear-text in logs. An attacker can retrieve them and bypass the authentication mechanism. As for the affected products/models/versions, see the reference URL.	2024-06-14	4.7	CVE-2024-27179
Trellix--Intrusion Prevention System (IPS) Manager	A vulnerability in the IPS Manager, Central Manager, and Local Manager communication workflow allows an attacker to control the destination of a request by manipulating the parameter, thereby leveraging sensitive information.	2024-06-14	6.8	CVE-2024-5731
Trellix--Trellix EDR UI (XConsole)	An Cross site scripting vulnerability in the EDR XConsole before this release allowed an attacker to potentially leverage an XSS/HTML-Injection using command line variables. A malicious threat actor could execute commands on the victim's browser for sending carefully crafted malicious links to the EDR XConsole end user.	2024-06-13	4.1	CVE-2024-4176
Trend Micro, Inc.--Trend Micro Apex One	A link following vulnerability in the Trend Micro Apex One and Apex One as a Service Damage Cleanup Engine could allow a local attacker to create a denial-of-service condition on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2024-06-10	6.1	CVE-2024-36306
Trend Micro, Inc.--Trend Micro Apex One	A security agent link following vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to disclose sensitive information about the agent on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2024-06-10	4.7	CVE-2024-36307
Trend Micro, Inc.--Trend Micro InterScan Web Security Virtual Appliance	A cross-site scripting (XSS) vulnerability in Trend Micro InterScan Web Security Virtual Appliance (IWSVA) 6.5 could allow an attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2024-06-10	5.4	CVE-2024-36359
Trend Micro, Inc.--Trend Micro VPN Proxy One Pro	Trend Micro VPN Proxy One Pro, version 5.8.1012 and below is vulnerable to an arbitrary file overwrite or create attack but is limited to local Denial of Service (DoS) and under specific conditions can lead to elevation of privileges.	2024-06-10	5.3	CVE-2024-36473
TreyWW--MyFinances	MyFinances is a web application for managing finances. MyFinances has a way to access other customer invoices while signed in as a user. This method allows an actor to access PII and financial information from another account. The vulnerability is fixed in 0.4.6.	2024-06-14	6.5	CVE-2024-37889
uniview -- nvr301-04s2-p4_firmware	Uniview NVR301-04S2-P4 is vulnerable to reflected cross-site scripting attack (XSS). An attacker could send a user a URL that if clicked on could execute malicious JavaScript in their browser. This vulnerability also requires authentication before it can be exploited, so the scope and severity is limited. Also, even if JavaScript is executed, no additional benefits are obtained.	2024-06-10	5.4	CVE-2024-3850
upunzipper_project -- upunzipper	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Ravidhu Dissanayake Upunzipper allows Path Traversal, File Manipulation.This issue affects Upunzipper: from n/a through 1.0.0.	2024-06-10	6.5	CVE-2024-35744
Vark--Pricing Deals for WooCommerce	Missing Authorization vulnerability in Vark Pricing Deals for WooCommerce.This issue affects Pricing Deals for WooCommerce: from n/a through 2.0.3.2.	2024-06-12	5.3	CVE-2023-41240

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vberkel--Schema App Structured Data	The Schema App Structured Data plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.2.0. This is due to missing or incorrect nonce validation on the MarkUpdate function. This makes it possible for unauthenticated attackers to update and delete post metadata via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-06-14	4.3	CVE-2024-0892
Verint--WFO	Verint - CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	2024-06-13	6.1	CVE-2024-36395
vsourz1td--Advanced Contact form 7 DB	The Advanced Contact form 7 DB plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.0.2 via the wp-content/uploads/advanced-cf7-upload directory. This makes it possible for unauthenticated attackers to extract sensitive data uploaded via this plugin through a form.	2024-06-11	5.3	CVE-2024-3723
vsourz1td--Advanced Contact form 7 DB	The Advanced Contact form 7 DB plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'vsz_cf7_export_to_excel' function in versions up to, and including, 2.0.2. This makes it possible for unauthenticated attackers to download the entry data for submitted forms.	2024-06-11	5.3	CVE-2024-4319
WebCodingPlace--Product Expiry for WooCommerce	Missing Authorization vulnerability in WebCodingPlace Product Expiry for WooCommerce.This issue affects Product Expiry for WooCommerce: from n/a through 2.5.	2024-06-11	5.4	CVE-2023-52179
webtechstreet--Elementor Addon Elements	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Twitter Widget in all versions up to, and including, 1.13.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-12	5.4	CVE-2024-2092
WebToffee--WordPress Backup & Migration	Missing Authorization vulnerability in WebToffee WordPress Backup & Migration.This issue affects WordPress Backup & Migration: from n/a through 1.4.3.	2024-06-11	5.4	CVE-2023-52183
weDevs--weDocs	Missing Authorization vulnerability in weDevs weDocs.This issue affects weDocs: from n/a through 2.1.4.	2024-06-11	5.3	CVE-2024-34442
weDevs--weMail	Missing Authorization vulnerability in weDevs weMail.This issue affects weMail: from n/a through 1.14.2.	2024-06-11	5.3	CVE-2024-34822
weDevs--WooCommerce Conversion Tracking	Missing Authorization vulnerability in weDevs WooCommerce Conversion Tracking.This issue affects WooCommerce Conversion Tracking: from n/a through 2.0.11.	2024-06-11	4.3	CVE-2023-52217
weForms--weForms	Missing Authorization vulnerability in weForms.This issue affects weForms: from n/a through 1.6.18.	2024-06-12	4.3	CVE-2023-51524
Welcart Inc.--Welcart e-Commerce	Missing Authorization vulnerability in Welcart Inc. Welcart e-Commerce.This issue affects Welcart e-Commerce: from n/a through 2.9.14.	2024-06-11	5.4	CVE-2024-32144

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Woo--WooCommerce Canada Post Shipping	Missing Authorization vulnerability in Woo WooCommerce Canada Post Shipping.This issue affects WooCommerce Canada Post Shipping: from n/a through 2.8.3.	2024-06-11	5.3	CVE-2023-51498
Woo--WooCommerce Product Vendors	Missing Authorization vulnerability in Woo WooCommerce Product Vendors.This issue affects WooCommerce Product Vendors: from n/a through 2.2.2.	2024-06-11	5.3	CVE-2023-52186
Woo--WooCommerce Ship to Multiple Addresses	Missing Authorization vulnerability in Woo WooCommerce Ship to Multiple Addresses.This issue affects WooCommerce Ship to Multiple Addresses: from n/a through 3.8.9.	2024-06-14	5.4	CVE-2023-51497
Woo--WooCommerce Warranty Requests	Missing Authorization vulnerability in Woo WooCommerce Warranty Requests.This issue affects WooCommerce Warranty Requests: from n/a through 2.2.7.	2024-06-14	6.5	CVE-2023-51495
Woo--WooCommerce Warranty Requests	Missing Authorization vulnerability in Woo WooCommerce Warranty Requests.This issue affects WooCommerce Warranty Requests: from n/a through 2.2.7.	2024-06-14	5.3	CVE-2023-51496
woocommerce--woocommerce	WooCommerce is an open-source e-commerce platform built on WordPress. A vulnerability introduced in WooCommerce 8.8 allows for cross-site scripting. A bad actor can manipulate a link to include malicious HTML & JavaScript content. While the content is not saved to the database, the links may be sent to victims for malicious purposes. The injected JavaScript could hijack content & data stored in the browser, including the session. The URL content is read through the `Sourcebuster.js` library and then inserted without proper sanitization to the classic checkout and registration forms. Versions 8.8.5 and 8.9.3 contain a patch for the issue. As a workaround, one may disable the Order Attribution feature.	2024-06-12	5.4	CVE-2024-37297
WP EasyCart--WP EasyCart	Missing Authorization vulnerability in WP EasyCart.This issue affects WP EasyCart: from n/a through 5.5.19.	2024-06-11	5.3	CVE-2024-35667
WP OnlineSupport, Essential Plugin--Preloader for Website	Missing Authorization vulnerability in WP OnlineSupport, Essential Plugin Preloader for Website.This issue affects Preloader for Website: from n/a through 1.2.2.	2024-06-11	5.3	CVE-2023-48273
wpbakery--WPBakery Visual Composer	The WPBakery Visual Composer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the link attribute within the vc_single_image shortcode in all versions up to, and including, 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.	2024-06-13	6.4	CVE-2024-5265
wpdevteam--EmbedPress Embed PDF, Google Docs, Vimeo, Wistia, Embed YouTube Videos, Audios, Maps & Embed	The EmbedPress - Embed PDF, YouTube, Google Docs, Vimeo, Wistia Videos, Audios, Maps & Any Documents in Gutenberg & Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the PDF Widget URL in all versions up to, and including, 3.9.10 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.	2024-06-13	6.4	CVE-2024-1565

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Any Documents in Gutenberg & Elementor				
wpdevteam--Essential Addons for Elementor Best Elementor Templates, Widgets, Kits & WooCommerce Builders	The Essential Addons for Elementor - Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'custom_js' parameter in all versions up to, and including, 5.9.23 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.	2024-06-11	6.4	CVE-2024-5189
WPEverest--Everest Forms	Missing Authorization vulnerability in WPEverest Everest Forms.This issue affects Everest Forms: from n/a through 2.0.3.	2024-06-14	5.3	CVE-2023-51377
wpgmaps--WP Go Maps (formerly WP Google Maps)	The WP Go Maps (formerly WP Google Maps) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Custom JS option in versions up to, and including, 9.0.38. This makes it possible for authenticated attackers that have been explicitly granted permissions by an administrator, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Version 9.0.39 adds a caution to make administrators aware of the possibility for abuse if permissions are granted to lower-level users.	2024-06-14	6.4	CVE-2024-5994
WPManageNinja LLC--Ninja Tables	Missing Authorization vulnerability in WPManageNinja LLC Ninja Tables.This issue affects Ninja Tables: from n/a through 5.0.5.	2024-06-14	5.3	CVE-2024-23504
WPManageNinja LLC--Ninja Tables	Missing Authorization vulnerability in WPManageNinja LLC Ninja Tables.This issue affects Ninja Tables: from n/a through 5.0.6.	2024-06-11	4.3	CVE-2024-23503
wpmet--ElementsKit Pro	The ElementsKit Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Motion Text and Table widgets in all versions up to, and including, 3.6.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-15	6.4	CVE-2024-5263
Wpmet--WP Fundraising Donation and Crowdfunding Platform	Missing Authorization vulnerability in Wpmet WP Fundraising Donation and Crowdfunding Platform.This issue affects WP Fundraising Donation and Crowdfunding Platform: from n/a through 1.6.4.	2024-06-11	5.3	CVE-2024-34758
WPWeb--WooCommerce - Social Login	The WooCommerce - Social Login plugin for WordPress is vulnerable to Email Verification in all versions up to, and including, 2.6.2 via the use of insufficiently random activation code. This makes it possible for unauthenticated attackers to bypass the email verification.	2024-06-15	6.5	CVE-2024-5868
WriterSystem--WooCommerce Easy Duplicate Product	Missing Authorization vulnerability in WriterSystem WooCommerce Easy Duplicate Product.This issue affects WooCommerce Easy Duplicate Product: from n/a through 0.3.0.7.	2024-06-14	4.3	CVE-2023-51523

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
XjSv--Cooked	The Cooked Pro recipe plugin for WordPress is vulnerable to Persistent Cross-Site Scripting (XSS) via the `_recipe_settings[post_title]` parameter in versions up to, and including, 1.7.15.4 due to insufficient input sanitization and output escaping. This vulnerability allows authenticated attackers with contributor-level access and above to inject arbitrary web scripts in pages that will execute whenever a user accesses a compromised page. A patch is available at commit 8cf88f334ccbf11134080bbb655c66f1cfe77026 and will be part of version 1.8.0.	2024-06-13	5.4	CVE-2024-37308
xpeedstudio--MetForm Contact Form, Survey, Quiz, & Custom Form Builder for Elementor	The MetForm - Contact Form, Survey, Quiz, & Custom Form Builder for Elementor plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 3.8.8 via the 'handle_file' function. This can allow unauthenticated attackers to extract sensitive data, such as Personally Identifiable Information, from files uploaded by users.	2024-06-11	5.3	CVE-2024-4266
yithemes --yith_woocommerce_product_add-ons	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in YITH YITH WooCommerce Product Add-Ons allows Code Injection.This issue affects YITH WooCommerce Product Add-Ons: from n/a through 4.9.2.	2024-06-10	5.3	CVE-2024-35680
Yoast--Yoast SEO Premium	Missing Authorization vulnerability in Yoast Yoast SEO Premium.This issue affects Yoast SEO Premium: from n/a through 20.4.	2024-06-11	5.3	CVE-2023-28775
yotuwp--Video Gallery YouTube Playlist, Channel Gallery by YotuWP	The Video Gallery - YouTube Playlist, Channel Gallery by YotuWP plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.3.13 via the display function. This makes it possible for authenticated attackers, with contributor access and higher, to include and execute arbitrary php files 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.	2024-06-15	6.4	CVE-2024-4551
5 Star Plugins--Easy Age Verify	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in 5 Star Plugins Easy Age Verify allows Stored XSS.This issue affects Easy Age Verify: from n/a through 1.8.2.	2024-06-21	5.9	CVE-2024-35757
A WP Life--Event Management Tickets Booking	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in A WP Life Event Management Tickets Booking.This issue affects Event Management Tickets Booking: from n/a through 1.4.0.	2024-06-21	5.3	CVE-2024-5059
ABB--800xA Base	Improper Input Validation vulnerability in ABB 800xA Base. An attacker who successfully exploited this vulnerability could cause services to crash by sending specifically crafted messages. This issue affects 800xA Base: from 6.0.0 through 6.1.1-2.	2024-06-21	5.7	CVE-2024-3036
Absolute Software--Secure Access	There is a cross-site scripting vulnerability in the policy management UI of Absolute Secure Access prior to version 13.06. Attackers can interfere with a system administrator's use of the policy management UI when the attacker convinces the victim administrator to follow a crafted link to the vulnerable component while the attacking administrator is authenticated to the console. The scope is unchanged, there is no loss of confidentiality. Impact to system integrity is high, impact to system availability is none.	2024-06-20	6.5	CVE-2024-37350
Absolute Software--Secure Access	There is a cross-site scripting vulnerability in the Secure Access administrative UI of Absolute Secure Access prior to version 13.06. Attackers can pass a limited-length script to the administrative UI which is then stored where an administrator can access it. The scope is unchanged, there is no loss of confidentiality. Impact to system availability is none, impact to system integrity is high	2024-06-20	5.3	CVE-2024-37345

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Absolute Software--Secure Access	There is a cross-site scripting vulnerability in the Secure Access administrative console of Absolute Secure Access prior to version 13.06. Attackers with valid tunnel credentials can pass a limited-length script to the administrative console which is then temporarily stored where an administrator using a non-default configuration could click on it while the attacker has a valid tunnel session with the server. The scope is unchanged, there is no loss of confidentiality. Impact to system availability is none, impact to system integrity is high.	2024-06-20	4.8	CVE-2024-37343
Absolute Software--Secure Access	There is a cross-site scripting vulnerability in the Policy management UI of Absolute Secure Access prior to version 13.06. Attackers with system administrator permissions can interfere with another system administrator's use of the policy management UI when the administrators are editing the same policy object. The scope is unchanged, there is no loss of confidentiality. Impact to system availability is none, impact to system integrity is high.	2024-06-20	4.5	CVE-2024-37344
Absolute Software--Secure Access	There is an insufficient input validation vulnerability in the Warehouse component of Absolute Secure Access prior to 13.06. Attackers with system administrator permissions can impair the availability of certain elements of the Secure Access administrative UI by writing invalid data to the warehouse over the network. There is no loss of warehouse integrity or confidentiality, the security scope is unchanged. Loss of availability is high.	2024-06-20	4.9	CVE-2024-37346
Absolute Software--Secure Access	There is a cross-site scripting vulnerability in the pool configuration component of the management UI of Absolute Secure Access prior to 13.06. Attackers with system administrator permissions can pass a limited length script to be run by another administrator. The scope is unchanged, there is no loss of confidentiality. Impact to system integrity is high, impact to system availability is none.	2024-06-20	4.5	CVE-2024-37347
Absolute Software--Secure Access	There is a cross-site scripting vulnerability in the management UI of Absolute Secure Access prior to version 13.06. Attackers with system administrator permissions can interfere with another system administrator's use of the management UI when the second administrator later edits the same management object. This vulnerability is distinct from CVE-2024-37349 and CVE-2024-37351. The scope is unchanged, there is no loss of confidentiality. Impact to system integrity is high, impact to system availability is none.	2024-06-20	4.5	CVE-2024-37348
Absolute Software--Secure Access	There is a cross-site scripting vulnerability in the management UI of Absolute Secure Access prior to version 13.06. Attackers with system administrator permissions can interfere with other system administrator's use of the management UI when the victim administrator edits the same management object. This vulnerability is distinct from CVE-2024-37348 and CVE-2024-37351. The scope is unchanged, there is no loss of confidentiality. Impact to system integrity is high, impact to system availability is none.	2024-06-20	4.5	CVE-2024-37349
Absolute Software--Secure Access	There is a cross-site scripting vulnerability in the management UI of Absolute Secure Access prior to version 13.06. Attackers with system administrator permissions can interfere with other system administrator's use of the management UI when the second administrator later edits the same management object. This vulnerability is distinct from CVE-2024-37348 and CVE-2024-37349. The scope is unchanged, there is no loss of confidentiality. Impact to system integrity is high, impact to system availability is none.	2024-06-20	4.5	CVE-2024-37351
Absolute Software--Secure Access	There is a cross-site scripting vulnerability in the management UI of Absolute Secure Access prior to version 13.06 that allows attackers with system administrator permissions to interfere with other system administrators' use of the management UI when the second administrator accesses the vulnerable page. The scope is unchanged, there is no loss of confidentiality. Impact to system integrity is high, impact to system availability is none.	2024-06-20	4.5	CVE-2024-37352
ali2woo--AliExpress	The AliExpress Dropshipping with AliNext Lite plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on several functions in the	2024-06-19	6.3	CVE-2024-4450

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Dropshipping with AliNext Lite	ImportAjaxController.php file in all versions up to, and including, 3.3.5. This makes it possible for authenticated attackers, with subscriber-level access and above, to perform several actions like importing and modifying products.			
ameliabooking--Booking for Appointments and Events Calendar Amelia	The Booking for Appointments and Events Calendar - Amelia plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.1.5 (and 7.5.1 for the Pro version) 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.	2024-06-21	4.4	CVE-2024-6225
Andy Moyle--Church Admin	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Andy Moyle Church Admin allows Stored XSS.This issue affects Church Admin: from n/a through 4.4.4.	2024-06-21	6.5	CVE-2024-35764
Apache Software Foundation--Apache Superset	Improper Input Validation vulnerability in Apache Superset, allows for an authenticated attacker to create a MariaDB connection with local_infile enabled. If both the MariaDB server (off by default) and the local mysql client on the web server are set to allow for local infile, it's possible for the attacker to execute a specific MySQL/MariaDB SQL command that is able to read files from the server and insert their content on a MariaDB database table.This issue affects Apache Superset: before 3.1.3 and version 4.0.0 Users are recommended to upgrade to version 4.0.1 or 3.1.3, which fixes the issue.	2024-06-20	6.8	CVE-2024-34693
armember--ARMember Premium Membership Plugin, Content Restriction, Member Levels, User Profile & User signup	The ARMember Premium plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 6.7. This is due to incorrectly implemented nonce validation function on multiple functions. This makes it possible for unauthenticated attackers to modify, or delete user meta and plugin options which can lead to limited privilege escalation.	2024-06-22	6.3	CVE-2024-5596
Artbees--JupiterX Core	Missing Authorization vulnerability in Artbees JupiterX Core.This issue affects JupiterX Core: from 3.0.0 through 3.3.0.	2024-06-19	5.4	CVE-2023-38394
aspengrovestudios--Replace Image	The Replace Image plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.1.10 via the image replacement functionality due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Author-level access and above, to replace images uploaded by higher level users such as admins.	2024-06-19	4.3	CVE-2024-4873
auburnforest--Blogmentor Blog Layouts for Elementor	The Blogmentor - Blog Layouts for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'pagination_style' parameter in all versions up to, and including, 1.5 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.	2024-06-19	6.4	CVE-2024-4623
Automattic--Jetpack	Missing Authorization vulnerability in Automattic Jetpack.This issue affects Jetpack: from n/a before 12.7.	2024-06-19	4.3	CVE-2023-47788
averta--Master Slider Responsive	The Master Slider - Responsive Touch Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ms_layer' shortcode in all versions up to, and including, 3.9.10 due to insufficient input sanitization and output escaping on the 'css_id' user supplied attribute. This makes it possible for authenticated	2024-06-18	6.4	CVE-2024-4375

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Touch Slider	attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
Averta--Master Slider	Cross-Site Request Forgery (CSRF) vulnerability in Averta Master Slider.This issue affects Master Slider: from n/a through 3.9.10.	2024-06-19	4.3	CVE-2023-50900
averta--Slider & Popup Builder by Depicter Add Image Slider, Carousel Slider, Exit Intent Popup, Popup Modal, Coupon Popup, Post Slider Carousel	The Slider and Carousel slider by Depicter plugin for WordPress is vulnerable to Arbitrary Nonce Generation in all versions up to, and including, 3.0.2. This makes it possible for authenticated attackers with contributor access and above, to generate a valid nonce for any WordPress action/function. This could be used to invoke functionality that is protected only by nonce checks.	2024-06-20	6.5	CVE-2024-4390
Axis Communications AB--AXIS OS	Johan FagerstrÃƒÂ¶m, member of the AXIS OS Bug Bounty Program, has found that a O3C feature may expose sensitive traffic between the client (Axis device) and (O3C) server. If O3C is not being used this flaw does not apply. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution.	2024-06-18	5.3	CVE-2024-0066 product-security@axis.com
blazethemes--Digital Newspaper	Cross-Site Request Forgery (CSRF) vulnerability in blazethemes Digital Newspaper.This issue affects Digital Newspaper: from n/a through 1.1.5.	2024-06-21	4.3	CVE-2024-37198
Brainstorm Force--Astra Bulk Edit	Missing Authorization vulnerability in Brainstorm Force Astra Bulk Edit.This issue affects Astra Bulk Edit: from n/a through 1.2.7.	2024-06-19	5.4	CVE-2023-44148
Brainstorm Force--Pre-Publish Checklist	Missing Authorization vulnerability in Brainstorm Force Pre-Publish Checklist.This issue affects Pre-Publish Checklist: from n/a through 1.1.1.	2024-06-19	5.4	CVE-2023-44151
Brainstorm Force--Premium Starter Templates	Missing Authorization vulnerability in Brainstorm Force Premium Starter Templates, Brainstorm Force Starter Templates astra-sites.This issue affects Premium Starter Templates: from n/a through 3.2.5; Starter Templates: from n/a through 3.2.5.	2024-06-19	6.5	CVE-2023-41805
Brainstorm Force--Spectra	Missing Authorization vulnerability in Brainstorm Force Spectra.This issue affects Spectra: from n/a through 2.6.6.	2024-06-19	5.4	CVE-2023-36676
brechtvds--WP Recipe Maker	The WP Recipe Maker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's [wprm-recipe-instructions] and [wprm-recipe-ingredients] shortcodes in all versions up to, and including, 9.1.0 due to insufficient restrictions on the 'group_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.	2024-06-19	6.4	CVE-2024-0383
BricksBuilder--Bricks Builder	The Bricks Builder plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.9.8 via the postId parameter due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Contributor-level access and above, to modify posts and pages created by other users including admins. As a requirement for this, an admin would have to enable access to the editor specifically for such a user or enable it for all users with a certain user account type.	2024-06-22	4.3	CVE-2024-4874

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cartflowswp--WooCommerce Checkout & Funnel Builder by CartFlows Create High Converting Stores For WooCommerce	The WooCommerce Checkout & Funnel Builder by CartFlows - Create High Converting Stores For WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'custom_upload_mimes' function in versions up to, and including, 2.0.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-19	6.4	CVE-2024-4632
Checkmk GmbH--Checkmk	Stored XSS in inventory tree rendering in Checkmk before 2.3.0p7, 2.2.0p28, 2.1.0p45 and 2.0.0 (EOL)	2024-06-17	6.5	CVE-2024-5741
convertkit--ConvertKit Email Newsletter, Email Marketing, Subscribers and Landing Pages	The ConvertKit - Email Newsletter, Email Marketing, Subscribers and Landing Pages plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the tag_subscriber function in all versions up to, and including, 2.4.9. This makes it possible for unauthenticated attackers to subscribe users to tags. Financial damages may occur to site owners if their API quota is exceeded.	2024-06-21	5.3	CVE-2024-3961
cozmoslabs--User Profile Picture	The User Profile Picture plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.6.1 via the 'rest_api_change_profile_image' function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Author-level access and above, to update the profile picture of any user.	2024-06-21	4.3	CVE-2024-5639
Crocoblock--JetElements For Elementor	Missing Authorization vulnerability in Crocoblock JetElements For Elementor.This issue affects JetElements For Elementor: from n/a through 2.6.13.	2024-06-19	6.3	CVE-2023-48761
Cryout Creations--Serious Slider	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Cryout Creations Serious Slider allows Stored XSS.This issue affects Serious Slider: from n/a through 1.2.4.	2024-06-21	6.5	CVE-2024-35762
D-Link--G403	Certain models of D-Link wireless routers have a path traversal vulnerability. Unauthenticated attackers on the same local area network can read arbitrary system files by manipulating the URL.	2024-06-17	6.5	CVE-2024-6044
Darteweb--DImage 360	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in D'arteweb DImage 360 allows Stored XSS.This issue affects DImage 360: from n/a through 2.0.	2024-06-21	6.5	CVE-2024-35774
Dave Kiss--Vimeography: Vimeo Video Gallery WordPress Plugin	Cross-Site Request Forgery (CSRF) vulnerability in Dave Kiss Vimeography: Vimeo Video Gallery WordPress Plugin.This issue affects Vimeography: Vimeo Video Gallery WordPress Plugin: from n/a through 2.4.1.	2024-06-21	4.3	CVE-2024-35770
drakkan--sftpgo	SFTPGo is a full-featured and highly configurable SFTP, HTTP/S, FTP/S and WebDAV server - S3, Google Cloud Storage, Azure Blob. SFTPGo WebAdmin and WebClient support password reset. This feature is disabled in the default configuration. In SFTPGo versions prior to v2.6.1, if the feature is enabled, even users with access restrictions (e.g. expired) can reset their password and log in. Users are advised to upgrade to version 2.6.1. Users unable to upgrade may keep the password reset feature disabled or set a blank email address for users and admins with access restrictions so they cannot receive the email with the reset code and exploit the vulnerability.	2024-06-20	5.4	CVE-2024-37897

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Elastic--Kibana	A high-privileged user, allowed to create custom osquery packs 17 could affect the availability of Kibana by uploading a maliciously crafted osquery pack.	2024-06-19	4.9	CVE-2024-23443
Elegant Themes--Divi	The Divi theme for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 4.25.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-18	6.4	CVE-2024-5533
Elementor--Elementor Pro	Missing Authorization vulnerability in Elementor Elementor Pro.This issue affects Elementor Pro: from n/a through 3.13.0.	2024-06-19	6.5	CVE-2023-35050
embedsocial--EmbedSocial Social Media Feeds, Reviews and Galleries	The EmbedSocial - Social Media Feeds, Reviews and Galleries plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'embedsocial_reviews' shortcode in all versions up to, and including, 1.1.29 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.	2024-06-19	6.4	CVE-2024-3984
Exeebit--phpinfo() WP	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Exeebit phpinfo() WP.This issue affects phpinfo() WP: from n/a through 5.0.	2024-06-21	5.3	CVE-2024-35776
extendthemes--Materialis	The Materialis theme for WordPress is vulnerable to limited arbitrary options updates in versions up to, and including, 1.1.24. This is due to missing authorization checks on the companion_disable_popup() function called via an AJAX action. This makes it possible for authenticated attackers, with minimal permissions such as subscribers, to modify any option on the site to a numerical value.	2024-06-20	6.5	CVE-2023-3204
EZ-Suite--EZ-Partner	A vulnerability classified as problematic has been found in EZ-Suite EZ-Partner 5. Affected is an unknown function of the component Forgot Password Handler. The manipulation leads to basic cross site scripting. It is possible to launch the attack remotely. VDB-269154 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-20	4.3	CVE-2024-6183
firefly-iii--firefly-iii	Firefly III is a free and open source personal finance manager. In affected versions an MFA bypass in the Firefly III OAuth flow may allow malicious users to bypass the MFA-check. This allows malicious users to use password spraying to gain access to Firefly III data using passwords stolen from other sources. As OAuth applications are easily enumerable using an incrementing id, an attacker could try sign an OAuth application up to a users profile quite easily if they have created one. The attacker would also need to know the victims username and password. This problem has been patched in Firefly III v6.1.17 and up. Users are advised to upgrade. Users unable to upgrade should Use a unique password for their Firefly III instance and store their password securely, i.e. in a password manager.	2024-06-17	5.9	CVE-2024-37893
florent73--WP Maintenance	The WP Maintenance plugin for WordPress is vulnerable to IP Address Spoofing in all versions up to, and including, 6.1.9.2 due to insufficient IP address validation and use of user-supplied HTTP headers as a primary method for IP retrieval. This makes it possible for unauthenticated attackers to bypass maintenance mode.	2024-06-19	5.3	CVE-2024-0789
fusionplugin--Table Addons for Elementor	The Table Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '_id' parameter in all versions up to, and including, 2.1.2 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.	2024-06-22	6.4	CVE-2024-4313

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
GamiPress--GamiPress	Cross-Site Request Forgery (CSRF) vulnerability in GamiPress.This issue affects GamiPress: from n/a through 2.5.6.	2024-06-19	5.4	CVE-2023-25697
garbowza--OSM Map Widget for Elementor	The OSM Map Widget for Elementor plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'id' parameter in all versions up to, and including, 1.2.2 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.	2024-06-19	6.4	CVE-2024-4663
Genexis--Tilgin Home Gateway	A vulnerability was found in Genexis Tilgin Home Gateway 322_AS0500-03_05_13_05. It has been classified as problematic. Affected is an unknown function of the file /vood/cgi-bin/vood_view.cgi?act=index&lang=EN# of the component Login. The manipulation of the argument errmsg leads to basic cross site scripting. It is possible to launch the attack remotely. VDB-268854 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-18	4.3	CVE-2024-6108
gVectors Team--wpForo Forum	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in gVectors Team wpForo Forum allows Content Spoofing.This issue affects wpForo Forum: from n/a through 2.0.9.	2024-06-21	4.3	CVE-2022-38055
Hennessey Digital--Attorney	Missing Authorization vulnerability in Hennessey Digital Attorney.This issue affects Attorney: from n/a through 3.	2024-06-19	6.5	CVE-2022-45832
itsourcecode--Tailoring Management System	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file addmeasurement.php. The manipulation of the argument id 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-268855.	2024-06-18	6.3	CVE-2024-6109
itsourcecode--Tailoring Management System	A vulnerability, which was classified as critical, was found in itsourcecode Tailoring Management System 1.0. Affected is an unknown function of the file editmeasurement.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-269166 is the identifier assigned to this vulnerability.	2024-06-20	6.3	CVE-2024-6194
itsourcecode--Tailoring Management System	A vulnerability has been found in itsourcecode Tailoring Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file orderadd.php. The manipulation of the argument customer 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-269167.	2024-06-20	6.3	CVE-2024-6195
jeffparker--YARPP Yet Another Related Posts Plugin	The YARPP - Yet Another Related Posts Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to and including 5.30.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2024-06-19	4.4	CVE-2023-6495
JetBrains--YouTrack	In JetBrains YouTrack before 2024.2.34646 user without appropriate permissions could enable the auto-attach option for workflows	2024-06-18	6.3	CVE-2024-38506

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
JetBrains--YouTrack	In JetBrains YouTrack before 2024.2.34646 user access token was sent to the third-party site	2024-06-18	5.3	CVE-2024-38505
JetBrains--YouTrack	In JetBrains YouTrack before 2024.2.34646 the Guest User Account was enabled for attaching files to articles	2024-06-18	4.3	CVE-2024-38504
jetmonsters--JetWidgets For Elementor	The JetWidgets For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'layout_type' and 'id' parameters in all versions up to, and including, 1.0.17 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.	2024-06-20	6.4	CVE-2024-4626
John West--Slideshow SE	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in John West Slideshow SE allows PHP Local File Inclusion.This issue affects Slideshow SE: from n/a through 2.5.17.	2024-06-21	6.5	CVE-2024-35778
John West--Slideshow SE	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in John West Slideshow SE allows Stored XSS.This issue affects Slideshow SE: from n/a through 2.5.17.	2024-06-21	5.9	CVE-2024-35769
kraftplugins--Wheel of Life: Coaching and Assessment Tool for Life Coach	The Wheel of Life: Coaching and Assessment Tool for Life Coach plugin for WordPress is vulnerable to unauthorized modification and loss of data due to a missing capability check on several functions in the AjaxFunctions.php file in all versions up to, and including, 1.1.7. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary posts and modify settings.	2024-06-20	5.4	CVE-2024-3627
lg -- supersign_cms	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in LG Electronics SuperSign CMS allows Reflected XSS.Ã, This issue affects SuperSign CMS: from 4.1.3 before < 4.3.1.	2024-06-20	6.1	CVE-2024-6177
lg -- supersign_cms	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LG Electronics SuperSign CMS allows Reflected XSS.Ã, This issue affects SuperSign CMS: from 4.1.3 before < 4.3.1.	2024-06-20	6.1	CVE-2024-6178
lg -- supersign_cms	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LG Electronics SuperSign CMS allows Reflected XSS.Ã, This issue affects SuperSign CMS: from 4.1.3 before < 4.3.1.	2024-06-20	6.1	CVE-2024-6179
lightningnetwork--lnd	The Lightning Network Daemon (lnd) - is a complete implementation of a Lightning Network node. A parsing vulnerability in lnd's onion processing logic and lead to a DoS vector due to excessive memory allocation. The issue was patched in lnd v0.17.0. Users should update to a version > v0.17.0 to be protected. Users unable to upgrade may set the `--rejecthtlc` CLI flag and also disable forwarding on channels via the `UpdateChanPolicyCommand`, or disable listening on a public network interface via the `--nolisten` flag as a mitigation.	2024-06-20	6.5	CVE-2024-38359
Live Composer Team--Page Builder: Live Composer	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Live Composer Team Page Builder: Live Composer allows Stored XSS.This issue affects Page Builder: Live Composer: from n/a through 1.5.42.	2024-06-21	6.5	CVE-2024-35779
Live Composer Team--Page Builder: Live Composer	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Live Composer Team Page Builder: Live Composer allows Stored XSS.This issue affects Page Builder: Live Composer: from n/a through 1.5.42.	2024-06-21	5.9	CVE-2024-35768

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lobehub--lobe-chat	Lobe Chat is an open-source LLMs/AI chat framework. In affected versions if an attacker can successfully authenticate through SSO/Access Code, they can obtain the real backend API Key by modifying the base URL to their own attack URL on the frontend and setting up a server-side request. This issue has been addressed in version 0.162.25. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-06-17	5.7	CVE-2024-37895
maxfoundry--MaxGalleria	The MaxGalleria plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's maxgallery_thumb shortcode in all versions up to, and including, 6.4.4 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.	2024-06-18	6.4	CVE-2024-5970
mgibbs189--Custom Field Suite	The Custom Field Suite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the the 'cfs[post_title]' parameter versions up to, and including, 2.6.7 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.	2024-06-20	6.4	CVE-2024-3558
Microsoft--Microsoft Edge (Chromium-based)	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-06-20	4.7	CVE-2024-38082
Microsoft--Microsoft Edge (Chromium-based)	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-06-20	4.3	CVE-2024-38093
n/a--GPAC	A vulnerability was found in GPAC 2.5-DEV-rev228-g11067ea92-master. It has been declared as problematic. This vulnerability affects the function xmt_node_end of the file src/scene_manager/loader_xmt.c of the component MP4Box. The manipulation leads to use after free. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The name of the patch is f4b3e4d2f91bc1749e7a924a8ab171af03a355a8/c1b9c794bad8f262c56f3cf690567980d96662f5. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-268792.	2024-06-17	5.3	CVE-2024-6064
n/a--n/a	Samsung Magician 8.0.0 on Windows allows an admin to escalate privileges by tampering with the directory and DLL files used during the installation process. This occurs because of an Untrusted Search Path.	2024-06-20	6.3	CVE-2024-36071
n/a--n/a	An issue was discovered in the friendlycaptcha_official (aka Integration of Friendly Captcha) extension before 0.1.4 for TYPO3. The extension fails to check the requirement of the captcha field in submitted form data, allowing a remote user to bypass the captcha check. This only affects the captcha integration for the ext:form extension.	2024-06-21	5.3	CVE-2024-38873
n/a--n/a	An issue was discovered in the events2 (aka Events 2) extension before 8.3.8 and 9.x before 9.0.6 for TYPO3. Missing access checks in the management plugin lead to an insecure direct object reference (IDOR) vulnerability with the potential to activate or delete various events for unauthenticated users.	2024-06-21	5.4	CVE-2024-38874
n/a--opencart/opencart	This affects versions of the package opencart/opencart from 4.0.0.0. An Arbitrary File Creation issue was identified via the database restoration functionality. By injecting PHP code into the database, an attacker with admin privileges can create a backup file with an arbitrary filename (including the extension), within	2024-06-22	6.6	CVE-2024-21519

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	/system/storage/backup. **Note:** It is less likely for the created file to be available within the web root, as part of the security recommendations for the application suggest moving the storage path outside of the web root.			
n/a--opencart/opencart	This affects versions of the package opencart/opencart from 4.0.0.0. A reflected XSS issue was identified in the filename parameter of the admin tool/log route. An attacker could obtain a user's token by tricking the user to click on a maliciously crafted URL. The user is then prompted to login and redirected again upon authentication with the payload automatically executing. If the attacked user has admin privileges, this vulnerability could be used as the start of a chain of exploits like Zip Slip or arbitrary file write vulnerabilities in the admin functionality. **Notes:** 1) This is only exploitable if the attacker knows the name or path of the admin directory. The name of the directory is "admin" by default but there is a pop-up in the dashboard warning users to rename it. 2) The fix for this vulnerability is incomplete. The redirect is removed so that it is not possible for an attacker to control the redirect post admin login anymore, but it is still possible to exploit this issue in admin if the user is authenticated as an admin already.	2024-06-22	4.2	CVE-2024-21515
n/a--opencart/opencart	This affects versions of the package opencart/opencart from 4.0.0.0. A reflected XSS issue was identified in the directory parameter of admin common/filemanager.list route. An attacker could obtain a user's token by tricking the user to click on a maliciously crafted URL. The user is then prompted to login and redirected again upon authentication with the payload automatically executing. If the attacked user has admin privileges, this vulnerability could be used as the start of a chain of exploits like Zip Slip or arbitrary file write vulnerabilities in the admin functionality. **Notes:** 1) This is only exploitable if the attacker knows the name or path of the admin directory. The name of the directory is "admin" by default but there is a pop-up in the dashboard warning users to rename it. 2) The fix for this vulnerability is incomplete. The redirect is removed so that it is not possible for an attacker to control the redirect post admin login anymore, but it is still possible to exploit this issue in admin if the user is authenticated as an admin already.	2024-06-22	4.2	CVE-2024-21516
n/a--opencart/opencart	This affects versions of the package opencart/opencart from 4.0.0.0. A reflected XSS issue was identified in the redirect parameter of customer account/login route. An attacker can inject arbitrary HTML and Javascript into the page response. As this vulnerability is present in the account functionality it could be used to target and attack customers of the OpenCart shop. **Notes:** 1) The fix for this vulnerability is incomplete	2024-06-22	4.2	CVE-2024-21517
n/a--Pear Admin Boot	A vulnerability was found in Pear Admin Boot up to 2.0.2 and classified as critical. This issue affects the function getDictItems of the file /system/dictData/getDictItems/. The manipulation with the input ,user(),1,1 leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-269375.	2024-06-21	6.3	CVE-2024-6241
n/a--PHPVibe	A vulnerability, which was classified as critical, was found in PHPVibe 11.0.46. Affected is an unknown function of the file /app/uploading/upload-mp3.php of the component Media Upload Page. The manipulation of the argument file leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-268824. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-18	6.3	CVE-2024-6083
n/a--spa-cartcms	A vulnerability, which was classified as problematic, has been found in spa-cartcms 1.9.0.6. This issue affects some unknown processing of the file /checkout of the component Checkout Page. The manipulation of the argument quantity with the input -10 leads to enforcement of behavioral workflow. The attack may be initiated	2024-06-18	5.3	CVE-2024-6128

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-268895.			
N/A--WP 2FA	Insertion of Sensitive Information into Log File vulnerability in WP 2FA allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects WP 2FA: from n/a through 2.6.3.	2024-06-21	5.3	CVE-2022-44587
Nikolay Strikhar--WordPress Form Builder Plugin Gutenberg Forms	Missing Authorization vulnerability in Nikolay Strikhar WordPress Form Builder Plugin - Gutenberg Forms.This issue affects WordPress Form Builder Plugin - Gutenberg Forms: from n/a through 2.2.8.3.	2024-06-21	6.5	CVE-2022-45803
Paid Memberships Pro--Paid Memberships Pro	Missing Authorization vulnerability in Paid Memberships Pro.This issue affects Paid Memberships Pro: from n/a through 1.2.3.	2024-06-19	5.4	CVE-2023-39990
Paradox Security Systems (Bahamas) Ltd.--IP150 Internet Module	The Paradox IP150 Internet Module in version 1.40.00 is vulnerable to Cross-Site Request Forgery (CSRF) attacks due to a lack of countermeasures and the use of the HTTP method `GET` to introduce changes in the system.	2024-06-19	6.8	CVE-2024-5676
Parsec Automation--TrackSYS	A vulnerability was found in Parsec Automation TrackSYS 11.x.x and classified as problematic. This issue affects some unknown processing of the file /TS/export/pagedefinition. The manipulation of the argument ID leads to direct request. 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-269159. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-20	5.3	CVE-2024-6188
pocketbase--pocketbase	Pocketbase is an open source web backend written in go. In affected versions a malicious user may be able to compromise other user accounts. In order to be exploited users must have both OAuth2 and Password auth methods enabled. A possible attack scenario could be: 1. a malicious actor register with the targeted user's email (it is unverified), 2. at some later point in time the targeted user stumble on your app and decides to sign-up with OAuth2 (_this step could be also initiated by the attacker by sending an invite email to the targeted user_), 3. on successful OAuth2 auth we search for an existing PocketBase user matching with the OAuth2 user's email and associate them, 4. because we haven't changed the password of the existing PocketBase user during the linking, the malicious actor has access to the targeted user account and will be able to login with the initially created email/password. To prevent this for happening we now reset the password for this specific case if the previously created user wasn't verified (an exception to this is if the linking is explicit/manual, aka. when you send `Authorization:TOKEN` with the OAuth2 auth call). Additionally to warn existing users we now send an email alert in case the user has logged in with password but has at least one OAuth2 account linked. The flow will be further improved with ongoing refactoring and we will start sending emails for "unrecognized device" logins (OTP and MFA is already implemented and will be available with the next v0.23.0 release in the near future). For the time being users are advised to update to version 0.22.14. There are no known workarounds for this vulnerability.	2024-06-18	5.4	CVE-2024-38351
ppfeufer--Grey Opaque	The Grey Opaque theme for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter within the theme's Download-Button shortcode in all versions up to, and including, 2.0.1 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.	2024-06-22	6.4	CVE-2024-5966

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Premium Addons--Premium Addons PRO	Missing Authorization vulnerability in Premium Addons Premium Addons PRO.This issue affects Premium Addons PRO: from n/a through 2.9.0.	2024-06-19	6.5	CVE-2023-37869
presscustomizr--Customizr	Cross-Site Request Forgery (CSRF) vulnerability in presscustomizr Customizr.This issue affects Customizr: from n/a through 4.4.21.	2024-06-21	4.3	CVE-2024-35771
presscustomizr--Hueman	Cross-Site Request Forgery (CSRF) vulnerability in presscustomizr Hueman.This issue affects Hueman: from n/a through 3.7.24.	2024-06-21	4.3	CVE-2024-35772
promolayerpopup builder--Pop ups, Exit intent popups, email popups, banners, bars, countdowns and cart savers Promolayer	The Pop ups, Exit intent popups, email popups, banners, bars, countdowns and cart savers - Promolayer plugin for WordPress is vulnerable to unauthorized plugin settings update due to a missing capability check on the disconnect_promolayer function in all versions up to, and including, 1.1.0. This makes it possible for authenticated attackers, with subscriber access or higher, to remove the Promolayer connection.	2024-06-20	4.3	CVE-2024-3602
QuadLayers--WooCommerce Checkout Manager	Missing Authorization vulnerability in QuadLayers WooCommerce Checkout Manager.This issue affects WooCommerce Checkout Manager: from n/a through 7.3.0.	2024-06-19	6.5	CVE-2023-47681
rainbowgeek--SEOPress On-site SEO	The SEOPress - On-site SEO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's social image URL in all versions up to, and including, 7.9 due to insufficient input sanitization and output escaping on user supplied image URLs. 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.	2024-06-20	6.4	CVE-2024-1168
Rara Theme--Book Landing Page	Cross-Site Request Forgery (CSRF) vulnerability in Rara Theme Book Landing Page.This issue affects Book Landing Page: from n/a through 1.2.3.	2024-06-21	4.3	CVE-2024-37230
Red Hat--Red Hat Directory Server 11	A denial of service vulnerability was found in the 389-ds-base LDAP server. This issue may allow an authenticated user to cause a server denial of service while attempting to log in with a user with a malformed hash in their password.	2024-06-18	5.7	CVE-2024-5953
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in the Poppler's Pdfinfo utility. This issue occurs when using -dests parameter with pdfinfo utility. By using certain malformed input files, an attacker could cause the utility to crash, leading to a denial of service.	2024-06-21	6.5	CVE-2024-6239
redlettuce--PDF Viewer for Elementor	The PDF Viewer for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the render function in all versions up to, and including, 2.9.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-18	6.4	CVE-2024-0845
robosoft--Photo Gallery, Images, Slider in Rbs Image Gallery	The Photo Gallery, Images, Slider in Rbs Image Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via an Image Title in all versions up to, and including, 3.2.19 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-19	6.4	CVE-2024-3894

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Ruijie--RG-UAC	A vulnerability classified as critical was found in Ruijie RG-UAC 1.0. Affected by this vulnerability is an unknown functionality of the file /view/systemConfig/reboot/reboot_commit.php. The manipulation of the argument servicename leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-269155. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-20	6.3	CVE-2024-6184
Ruijie--RG-UAC	A vulnerability, which was classified as critical, has been found in Ruijie RG-UAC 1.0. Affected by this issue is the function get_ip_addr_details of the file /view/dhcp/dhcpConfig/commit.php. The manipulation of the argument ethname leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-269156. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-20	6.3	CVE-2024-6185
Ruijie--RG-UAC	A vulnerability, which was classified as critical, was found in Ruijie RG-UAC 1.0. This affects an unknown part of the file /view/userAuthentication/SSO/commit.php. The manipulation of the argument ad_log_name leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-269157 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-20	6.3	CVE-2024-6186
Ruijie--RG-UAC	A vulnerability has been found in Ruijie RG-UAC 1.0 and classified as critical. This vulnerability affects unknown code of the file /view/vpn/autovpn/sub_commit.php. The manipulation of the argument key leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-269158 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-20	6.3	CVE-2024-6187
shaonsina--Sina Extension for Elementor (Slider, Gallery, Form, Modal, Data Table, Tab, Particle, Free Elementor Widgets & Elementor Templates)	The Sina Extension for Elementor (Slider, Gallery, Form, Modal, Data Table, Tab, Particle, Free Elementor Widgets & Elementor Templates) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter in all versions up to, and including, 3.5.4 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.	2024-06-20	6.4	CVE-2024-5036
shortpixel--WP SVG Images	The WP SVG Images plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'type' parameter in all versions up to, and including, 4.2 due to insufficient input sanitization. This makes it possible for authenticated attackers, with Author-level access and above, who have permissions to upload sanitized files, to bypass SVG sanitization and inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-21	6.4	CVE-2024-5945
SourceCodester--Best House Rental Management System	A vulnerability classified as critical has been found in SourceCodester Best House Rental Management System 1.0. Affected is an unknown function of the file payment_report.php. The manipulation of the argument month_of 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-268794 is the identifier assigned to this vulnerability.	2024-06-17	6.3	CVE-2024-6066
SourceCodester--Food Ordering Management	A vulnerability was found in SourceCodester Food Ordering Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file add-item.php. The manipulation of the argument price leads to sql injection.	2024-06-21	6.3	CVE-2024-6214

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
System	The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-269278 is the identifier assigned to this vulnerability.			
SourceCodester--Food Ordering Management System	A vulnerability was found in SourceCodester Food Ordering Management System up to 1.0. It has been rated as critical. This issue affects some unknown processing of the file view-ticket-admin.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-269279.	2024-06-21	6.3	CVE-2024-6215
SourceCodester--Food Ordering Management System	A vulnerability classified as critical has been found in SourceCodester Food Ordering Management System 1.0. Affected is an unknown function of the file add-users.php. The manipulation of the argument contact 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-269280.	2024-06-21	6.3	CVE-2024-6216
SourceCodester--Food Ordering Management System	A vulnerability classified as critical was found in SourceCodester Food Ordering Management System 1.0. Affected by this vulnerability is an unknown functionality of the file user-router.php. The manipulation of the argument 1_verified 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-269281 was assigned to this vulnerability.	2024-06-21	6.3	CVE-2024-6217
SourceCodester--Music Class Enrollment System	A vulnerability classified as critical was found in SourceCodester Music Class Enrollment System 1.0. Affected by this vulnerability is an unknown functionality of the file /mces/?p=class/view_class. The manipulation of the argument id 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-268795.	2024-06-17	6.3	CVE-2024-6067
sparklewpthemes--Sparkle Demo Importer	The Sparkle Demo Importer plugin for WordPress is vulnerable to unauthorized database reset and demo data import due to a missing capability check on the multiple functions in all versions up to and including 1.4.7. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete all posts, pages, and uploaded files, as well as download and install a limited set of demo plugins.	2024-06-22	6.5	CVE-2024-6120
stacklok--minder	Minder is an open source Software Supply Chain Security Platform. Minder's Git provider is vulnerable to a denial of service from a maliciously configured GitHub repository. The Git provider clones users repositories using the `github.com/go-git/go-git/v5` library on lines `L55-L89`. The Git provider does the following on the lines `L56-L62`. First, it sets the `CloneOptions`, specifying the url, the depth etc. It then validates the options. It then sets up an in-memory filesystem, to which it clones and Finally, it clones the repository. The `(g *Git) Clone()` method is vulnerable to a DoS attack: A Minder user can instruct Minder to clone a large repository which will exhaust memory and crash the Minder server. The root cause of this vulnerability is a combination of the following conditions: 1. Users can control the Git URL which Minder clones, 2. Minder does not enforce a size limit to the repository, 3. Minder clones the entire repository into memory. This issue has been addressed in commit `7979b43` which has been included in release version v0.0.52. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-06-18	5.7	CVE-2024-37904
startbooking--Scheduling Plugin Online Booking for WordPress	The Scheduling Plugin - Online Booking for WordPress plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'cbsb_disconnect_settings' function in all versions up to, and including, 3.5.10. This makes it possible for unauthenticated attackers to disconnect the plugin from the startbooking service and remove connection data.	2024-06-18	6.5	CVE-2024-1634

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
strangerstudios--Paid Memberships Pro Content Restriction, User Registration, & Paid Subscriptions	The Paid Memberships Pro - Content Restriction, User Registration, & Paid Subscriptions plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.12.10. This is due to missing or incorrect nonce validation on multiple functions. This makes it possible for unauthenticated attackers to subscribe to, modify, or cancel membership for a user via a forged request granted they can trick a user into performing an action such as clicking on a link.	2024-06-19	5.4	CVE-2024-1407
StylemixThemes--Cost Calculator Builder PRO	The Cost Calculator Builder PRO for WordPress is vulnerable to arbitrary email sending vulnerability in versions up to, and including, 3.1.75. This is due to insufficient limitations on the email recipient and the content in the 'send_pdf' and the 'send_pdf_front' functions which are reachable via AJAX. This makes it possible for unauthenticated attackers to send emails with any content to any recipient.	2024-06-19	5.8	CVE-2024-4787
surakrai--MIMO Woocommerce Order Tracking	The MIMO Woocommerce Order Tracking plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'mimo_update_provider' function in all versions up to, and including, 1.0.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update shipping provider information, including adding stored cross-site scripting.	2024-06-19	6.4	CVE-2024-5768
Theme Freesia--Excellent	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Theme Freesia Excellent allows Stored XSS.This issue affects Excellent: from n/a through 1.2.9.	2024-06-21	6.5	CVE-2024-35763
Theme Horse--Interface	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Theme Horse Interface allows Stored XSS.This issue affects Interface: from n/a through 3.1.0.	2024-06-21	6.5	CVE-2024-35758
ThemeFusion--Avada	Missing Authorization vulnerability in ThemeFusion Avada.This issue affects Avada: from n/a through 7.11.1.	2024-06-19	4.3	CVE-2023-39922
ThemeFusion--Fusion Builder	Missing Authorization vulnerability in ThemeFusion Fusion Builder.This issue affects Fusion Builder: from n/a through 3.11.1.	2024-06-19	5.4	CVE-2023-39310
themeisle--Orbit Fox by ThemeIsle	The Orbit Fox by ThemeIsle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Services and Post Type Grid widgets in all versions up to, and including, 2.10.34 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.	2024-06-22	6.4	CVE-2024-2484
ThemePunch OHG--Slider Revolution	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ThemePunch OHG Slider Revolution allows Stored XSS.This issue affects Slider Revolution: from n/a before 6.7.11.	2024-06-19	5.9	CVE-2024-34443
tickera--Tickera WordPress Event Ticketing	The Tickera - WordPress Event Ticketing plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the tc_dl_delete_tickets AJAX action in all versions up to, and including, 3.5.2.8. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete all tickets associated with events.	2024-06-18	4.3	CVE-2024-5860
tinymce--tinymce	TinyMCE is an open source rich text editor. A cross-site scripting (XSS) vulnerability was discovered in TinyMCE's content extraction code. When using the `noneditable_regexp` option, specially crafted HTML attributes containing malicious code were able to be executed when content was extracted from the editor. This vulnerability has been patched in TinyMCE 7.2.0, TinyMCE 6.8.4 and TinyMCE 5.11.0 LTS by ensuring that, when using the `noneditable_regexp` option, any content within an attribute is properly verified to match the configured regular	2024-06-19	6.1	CVE-2024-38356

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	expression before being added. Users are advised to upgrade. There are no known workarounds for this vulnerability.			
tinymce--tinymce	TinyMCE is an open source rich text editor. A cross-site scripting (XSS) vulnerability was discovered in TinyMCE's content parsing code. This allowed specially crafted noscript elements containing malicious code to be executed when that content was loaded into the editor. This vulnerability has been patched in TinyMCE 7.2.0, TinyMCE 6.8.4 and TinyMCE 5.11.0 LTS by ensuring that content within noscript elements are properly parsed. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-06-19	6.1	CVE-2024-38357
Tribulant--Newsletters	Cross Site Request Forgery (CSRF) vulnerability in Tribulant Newsletters.This issue affects Newsletters: from n/a through 4.9.7.	2024-06-21	4.3	CVE-2024-37227
ultimateblocks--Ultimate Blocks WordPress Blocks Plugin	The Ultimate Blocks - WordPress Blocks Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's tab anchor metabox in all versions up to, and including, 3.0.8 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.	2024-06-19	6.4	CVE-2023-6692
Uncanny Owl--Uncanny Automator Pro	Cross Site Request Forgery (CSRF) vulnerability in Uncanny Owl Uncanny Automator Pro.This issue affects Uncanny Automator Pro: from n/a through 5.3.	2024-06-21	5.4	CVE-2024-37118
Unknown--The Plus Addons for Elementor Page Builder	The The Plus Addons for Elementor Page Builder plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'forgoturl' attribute within the plugin's WP Login & Register widget in all versions up to, and including, 5.5.6 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.	2024-06-21	6.1	CVE-2024-5344
urllib3--urllib3	urllib3 is a user-friendly HTTP client library for Python. When using urllib3's proxy support with `ProxyManager`, the `Proxy-Authorization` header is only sent to the configured proxy, as expected. However, when sending HTTP requests *without* using urllib3's proxy support, it's possible to accidentally configure the `Proxy-Authorization` header even though it won't have any effect as the request is not using a forwarding proxy or a tunneling proxy. In those cases, urllib3 doesn't treat the `Proxy-Authorization` HTTP header as one carrying authentication material and thus doesn't strip the header on cross-origin redirects. Because this is a highly unlikely scenario, we believe the severity of this vulnerability is low for almost all users. Out of an abundance of caution urllib3 will automatically strip the `Proxy-Authorization` header during cross-origin redirects to avoid the small chance that users are doing this on accident. Users should use urllib3's proxy support or disable automatic redirects to achieve safe processing of the `Proxy-Authorization` header, but we still decided to strip the header by default in order to further protect users who aren't using the correct approach. We believe the number of usages affected by this advisory is low. It requires all of the following to be true to be exploited: 1. Setting the `Proxy-Authorization` header without using urllib3's built-in proxy support. 2. Not disabling HTTP redirects. 3. Either not using an HTTPS origin server or for the proxy or target origin to redirect to a malicious origin. Users are advised to update to either version 1.26.19 or version 2.2.2. Users unable to upgrade may use the `Proxy-Authorization` header with urllib3's `ProxyManager`, disable HTTP redirects using `redirects=False` when sending requests, or not user the `Proxy-Authorization` header as mitigations.	2024-06-17	4.4	CVE-2024-37891
UX-themes--Flatsome	The Flatsome theme for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 3.18.7 due to insufficient input sanitization and output escaping on user supplied attributes. This	2024-06-20	6.4	CVE-2024-5156

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			
UX-themes--Flatsome	The Flatsome theme for WordPress is vulnerable to Stored Cross-Site Scripting via the UX Countdown, Video Button, UX Video, UX Slider, UX Sidebar, and UX Payment Icons shortcodes in all versions up to, and including, 3.18.7 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.	2024-06-22	6.4	CVE-2024-5346
vCita--Online Booking & Scheduling Calendar for WordPress by vcita	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in vCita Online Booking & Scheduling Calendar for WordPress by vcita allows Stored XSS.This issue affects Online Booking & Scheduling Calendar for WordPress by vcita: from n/a through 4.4.0.	2024-06-21	6.5	CVE-2024-35761
vcita--Online Booking & Scheduling Calendar for WordPress by vcita	The Online Booking & Scheduling Calendar for WordPress by vcita plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'd' parameter in all versions up to, and including, 4.4.2 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.	2024-06-21	6.1	CVE-2024-5859
viitorcloudvc--Custom Product List Table	The Custom Product List Table plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.0.0. This is due to missing or incorrect nonce validation when modifying products. This makes it possible for unauthenticated attackers to add, delete, bulk edit, approve or cancel products via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-06-19	4.3	CVE-2024-4541
vowelweb--Ibtana WordPress Website Builder	The Ibtana - WordPress Website Builder plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ibtana_visual_editor_register_ajax_json_endpont' function in all versions up to, and including, 1.2.3.3. This makes it possible for unauthenticated attackers to update option values for reCAPTCHA keys on the WordPress site. This can be leveraged to bypass reCAPTCHA on the site.	2024-06-18	5.3	CVE-2024-5541
webhuntinfotech--Universal Slider	The Universal Slider plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.6.5 via deserialization of untrusted input 'fsl_get_gallery_value' function. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software. 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.	2024-06-19	5.4	CVE-2024-5649
wen-solutions--WP Child Theme Generator	The WP Child Theme Generator plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the wctg_easy_child_theme() function in all versions up to, and including, 1.1.1. This makes it possible for unauthenticated attackers to create a blank child theme and activate it cause the site to whitescreen.	2024-06-21	5.3	CVE-2024-3610
Westermo--L210-F2G Lynx	Plain text credentials and session ID can be captured with a network sniffer.	2024-06-20	5.7	CVE-2024-37183
wildweblab--Mosaic	The Mosaic theme for WordPress is vulnerable to Stored Cross-Site Scripting via the 'link' parameter within the theme's Button shortcode in all versions up to, and including, 1.7.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and	2024-06-22	6.4	CVE-2024-5965

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
Woo--AutomateWoo	Missing Authorization vulnerability in Woo AutomateWoo.This issue affects AutomateWoo: from n/a through 5.7.5.	2024-06-19	6.5	CVE-2023-36512
Woo--WooCommerce Ship to Multiple Addresses	Missing Authorization vulnerability in Woo WooCommerce Ship to Multiple Addresses.This issue affects WooCommerce Ship to Multiple Addresses: from n/a through 3.8.5.	2024-06-19	6.5	CVE-2023-37872
WP Job Portal--WP Job Portal	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Job Portal allows Stored XSS.This issue affects WP Job Portal: from n/a through 2.1.3.	2024-06-21	5.9	CVE-2024-35759
WP Job Portal--WP Job Portal	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Job Portal allows Stored XSS.This issue affects WP Job Portal: from n/a through 2.1.3.	2024-06-21	5.9	CVE-2024-35760
WP SCHEMA PRO--Schema Pro	Missing Authorization vulnerability in WP SCHEMA PRO Schema Pro.This issue affects Schema Pro: from n/a through 2.7.8.	2024-06-19	6.5	CVE-2023-36683
WPDeveloper--EmbedPress	Missing Authorization vulnerability in WPDeveloper EmbedPress.This issue affects EmbedPress: from n/a through 3.8.3.	2024-06-21	4.3	CVE-2023-51375
WPDeveloper--Typing Text	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPDeveloper Typing Text allows Stored XSS.This issue affects Typing Text: from n/a through 1.2.5.	2024-06-21	6.5	CVE-2024-5058
wpexpertsio--License Manager for WooCommerce	The License Manager for WooCommerce plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the showLicenseKey() and showAllLicenseKeys() functions in all versions up to, and including, 3.0.7. This makes it possible for authenticated attackers, with admin dashboard access (contributors by default due to WooCommerce) to view arbitrary decrypted license keys. The functions contain a referrer nonce check. However, these can be retrieved via the dashboard through the "license" JS variable.	2024-06-21	6.5	CVE-2024-1639
Wpmet--Elements kit Elementor addons	Missing Authorization vulnerability in Wpmet Elements kit Elementor addons.This issue affects Elements kit Elementor addons: from n/a through 2.9.0.	2024-06-19	4.3	CVE-2023-39993
wpmudev--Branda White Label WordPress, Custom Login Page Customizer	The Branda - White Label WordPress, Custom Login Page Customizer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'mime_types' parameter in all versions up to, and including, 3.4.17 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-21	6.4	CVE-2024-5191
wpmudev--Smush Image Optimization Optimize Images | Compress & Lazy Load Images | Convert WebP | Image CDN	The Smush plugin for WordPress is vulnerable to unauthorized deletion of the resmush list due to a missing capability check on the delete_resmush_list() function. This makes it possible for authenticated attackers, with minimal permissions such as a subscriber, to delete the resmush list for Nextgen or the Media Library.	2024-06-21	4.3	CVE-2023-3352

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wprepublic--Hide Dashboard Notifications	The Hide Dashboard Notifications plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'warning_notices_settings' function in all versions up to, and including, 1.3. This makes it possible for authenticated attackers, with contributor access and above, to modify the plugin's settings.	2024-06-21	4.3	CVE-2024-1955
Wpsoul--Greenshift animation and page builder blocks	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wpsoul Greenshift - animation and page builder blocks allows Stored XSS.This issue affects Greenshift - animation and page builder blocks: from n/a through 8.8.9.1.	2024-06-19	6.5	CVE-2024-35765
wpzoom--WPZOOM Addons for Elementor (Templates, Widgets)	The WPZOOM Addons for Elementor (Templates, Widgets) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' attribute within the plugin's Team Members widget in all versions up to, and including, 1.1.38 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.	2024-06-20	6.4	CVE-2024-5686
YAHMAN--Word Balloon	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in YAHMAN Word Balloon allows PHP Local File Inclusion.This issue affects Word Balloon: from n/a through 4.21.1.	2024-06-21	6.5	CVE-2024-35781
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 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.	2024-06-25	5.4	CVE-2024-34141
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 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.	2024-06-25	5.4	CVE-2024-34142
amans2k--Funnel Builder for WordPress by FunnelKit Customize WooCommerce Checkout Pages, Create Sales Funnels, Order Bumps & One Click Upsells	The Funnel Builder for WordPress by FunnelKit - Customize WooCommerce Checkout Pages, Create Sales Funnels, Order Bumps & One Click Upsells plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'mimes' parameter in all versions up to, and including, 3.3.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-29	6.4	CVE-2024-5192
anchorcms -- anchor_cms	Cross Site Scripting vulnerability in Anchor CMS v.0.12.7 allows a remote attacker to execute arbitrary code via a crafted .pdf file.	2024-06-24	6.1	CVE-2024-37732
Automattic--WordPress	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Automattic WordPress allows Stored XSS.This issue affects WordPress: from 6.5 through 6.5.4, from 6.4 through 6.4.4, from 6.3 through 6.3.4, from 6.2 through 6.2.5, from 6.1 through 6.1.6, from 6.0 through 6.0.8, from 5.9 through 5.9.9.	2024-06-25	6.5	CVE-2024-31111

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Automattic--WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Automattic WordPress allows Relative Path Traversal.This issue affects WordPress: from 6.5 through 6.5.4, from 6.4 through 6.4.4, from 6.3 through 6.3.4, from 6.2 through 6.2.5, from 6.1 through 6.1.6, from 6.0 through 6.0.8, from 5.9 through 5.9.9, from 5.8 through 5.8.9, from 5.7 through 5.7.11, from 5.6 through 5.6.13, from 5.5 through 5.5.14, from 5.4 through 5.4.15, from 5.3 through 5.3.17, from 5.2 through 5.2.20, from 5.1 through 5.1.18, from 5.0 through 5.0.21, from 4.9 through 4.9.25, from 4.8 through 4.8.24, from 4.7 through 4.7.28, from 4.6 through 4.6.28, from 4.5 through 4.5.31, from 4.4 through 4.4.32, from 4.3 through 4.3.33, from 4.2 through 4.2.37, from 4.1 through 4.1.40.	2024-06-25	5	CVE-2024-32111
awordpresslife--Portfolio Gallery Image Gallery Plugin	The Portfolio Gallery - Image Gallery Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'PFG' shortcode in all versions up to, and including, 1.6.4 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.	2024-06-27	6.4	CVE-2024-6262
bdthemes--Ultimate Post Kit Addons For Elementor (Post Grid, Post Carousel, Post Slider, Category List, Post Tabs, Timeline, Post Ticker, Tag Cloud)	The Ultimate Post Kit Addons For Elementor - (Post Grid, Post Carousel, Post Slider, Category List, Post Tabs, Timeline, Post Ticker, Tag Cloud) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter within the Social Count (Static) widget in all versions up to, and including, 3.11.7 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.	2024-06-28	6.4	CVE-2024-5662
berriai--berriai/litellm	berriai/litellm version 1.34.34 is vulnerable to improper access control in its team management functionality. This vulnerability allows attackers to perform unauthorized actions such as creating, updating, viewing, deleting, blocking, and unblocking any teams, as well as adding or deleting any member to or from any teams. The vulnerability stems from insufficient access control checks in various team management endpoints, enabling attackers to exploit these functionalities without proper authorization.	2024-06-27	5.3	CVE-2024-5710
bfintal--Stackable Page Builder Gutenberg Blocks	The Stackable - Page Builder Gutenberg Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'data-caption' parameter in all versions up to, and including, 3.13.1 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.	2024-06-28	6.4	CVE-2024-6296
bhagirath25--Floating Social Buttons	The Floating Social Buttons plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.5. This is due to missing or incorrect nonce validation on the floating_social_buttons_option() function. This makes it possible for unauthenticated attackers to update the plugins settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-06-29	6.1	CVE-2024-6405
bigbluebutton--bigbluebutton	BigBlueButton is an open-source virtual classroom designed to help teachers teach and learners learn. An attacker with a valid join link to a meeting can trick BigBlueButton into generating a signed join link with additional parameters. One of those parameters may be "role=moderator", allowing an attacker to join a meeting as moderator using a join link that was originally created for viewer access. This vulnerability has been patched in version(s) 2.6.18, 2.7.8 and 3.0.0-alpha.7.	2024-06-28	4.6	CVE-2024-38518

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Blossom Themes--BlossomThemes Email Newsletter	Server-Side Request Forgery (SSRF) vulnerability in Blossom Themes BlossomThemes Email Newsletter.This issue affects BlossomThemes Email Newsletter: from n/a through 2.2.6.	2024-06-26	4.4	CVE-2024-37098
brechtvds--Easy Affiliate Links	The Easy Affiliate Links plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the eafl_reset_settings AJAX action in all versions up to, and including, 3.7.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to reset the plugin's settings.	2024-06-28	4.3	CVE-2024-5864
brechtvds--Easy Image Collage	The Easy Image Collage plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the ajax_image_collage() function in all versions up to, and including, 1.13.5. This makes it possible for authenticated attackers, with Contributor-level access and above, to erase all of the content in arbitrary posts.	2024-06-28	5.4	CVE-2024-5863
britner--Gutenberg Blocks with AI by Kadence WP Page Builder Features	The Gutenberg Blocks with AI by Kadence WP - Page Builder Features plugin for WordPress is vulnerable to DOM-based Stored Cross-Site Scripting via HTML data attributes in all versions up to, and including, 3.2.45 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.	2024-06-29	6.4	CVE-2024-5819
Brocade--Fabric OS	A vulnerability in a password management API in Brocade Fabric OS versions before v9.2.1, v9.2.0b, v9.1.1d, and v8.2.3e prints sensitive information in log files. This could allow an authenticated user to view the server passwords for protocols such as scp and sftp. Detail. When the firmwaredownload command is incorrectly entered or points to an erroneous file, the firmware download log captures the failed command, including any password entered in the command line.	2024-06-26	5.9	CVE-2024-29954
Brocade--Fabric OS	A vulnerability in the web interface in Brocade Fabric OS before v9.2.1, v9.2.0b, and v9.1.1d prints encoded session passwords on session storage for Virtual Fabric platforms. This could allow an authenticated user to view other users' session encoded passwords.	2024-06-26	4.3	CVE-2024-29953
Canonical Ltd.--Ubuntu Advantage Desktop Pro	Marco Trevisan discovered that the Ubuntu Advantage Desktop Daemon, before version 1.12, leaks the Pro token to unprivileged users by passing the token as an argument in plaintext.	2024-06-27	5.9	CVE-2024-6388
carlosfazenda--Page and Post Clone	The Page and Post Clone plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 6.0 via the 'content_clone' function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Author-level access and above, to clone and read private posts.	2024-06-29	4.3	CVE-2024-5942
Checkmk GmbH--Checkmk	Stored XSS in some confirmation pop-ups in Checkmk before versions 2.3.0p7 and 2.2.0p28 allows Checkmk users to execute arbitrary scripts by injecting HTML elements into some user input fields that are shown in a confirmation pop-up.	2024-06-25	5.4	CVE-2024-28831
Checkmk GmbH--Checkmk	Stored XSS in the Crash Report page in Checkmk before versions 2.3.0p7, 2.2.0p28, 2.1.0p45, and 2.0.0 (EOL) allows users with permission to change Global Settings to execute arbitrary scripts by injecting HTML elements into the Crash Report URL in the Global Settings.	2024-06-25	4.8	CVE-2024-28832
CryoutCreations--Anima	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Anima allows Stored XSS.This issue affects Anima: from n/a through 1.4.1.	2024-06-26	6.5	CVE-2024-37248

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Dell--PowerEdge Platform	Dell PowerEdge Server BIOS contains an TOCTOU race condition vulnerability. A local low privileged attacker could potentially exploit this vulnerability to gain access to otherwise unauthorized resources.	2024-06-25	5.3	CVE-2024-0171
Dell--PowerProtect DD	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 contain a Server-Side Request Forgery (SSRF) vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to disclosure of information on the application or remote client.	2024-06-26	6.8	CVE-2024-29173
Dell--PowerProtect DD	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 contain an Improper Control of a Resource Through its Lifetime vulnerability in an admin operation. A remote low privileged attacker could potentially exploit this vulnerability, leading to temporary resource constraint of system application. Exploitation may lead to denial of service of the application.	2024-06-26	6.5	CVE-2024-37139
Dell--PowerProtect DD	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 contain a Stored Cross-Site Scripting Vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to the storage of malicious HTML or JavaScript codes in a trusted application data store. When a high privileged victim user accesses the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable web application. Exploitation may lead to information disclosure, session theft, or client-side request forgery	2024-06-26	5.9	CVE-2024-28973
Dell--PowerProtect DD	Dell PowerProtect Data Domain, versions prior to 7.13.0.0, LTS 7.7.5.40, LTS 7.10.1.30 contain an weak cryptographic algorithm vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to man-in-the-middle attack that exposes sensitive session information.	2024-06-26	5.9	CVE-2024-29175
Dell--PowerProtect DD	Dell Data Domain, versions prior to 7.13.0.0, LTS 7.7.5.30, LTS 7.10.1.20 contain an SQL Injection vulnerability. A local low privileged attacker could potentially exploit this vulnerability, leading to the execution of certain SQL commands on the application's backend database causing unauthorized access to application data.	2024-06-26	4.4	CVE-2024-29174
Dell--PowerProtect DD	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 on DDMC contain a relative path traversal vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to the application sending over an unauthorized file to the managed system.	2024-06-26	4.1	CVE-2024-37138
detheme -- dethemekit_for_elementor	The DethemeKit For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the URL parameter of the De Gallery widget in all versions up to and including 2.1.5 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 clicks on the injected link.	2024-06-27	5.4	CVE-2024-6283
devitemsllc--HT Mega Absolute Addons For Elementor	The HT Mega - Absolute Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Video player widget settings in all versions up to, and including, 2.5.5 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.	2024-06-26	6.4	CVE-2024-5173
devitemsllc--HT Mega Absolute Addons For Elementor	The HT Mega - Absolute Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple widgets in all versions up to, and including, 2.5.5 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.	2024-06-26	6.4	CVE-2024-5215
Dream-Theme--The7 Website and	The The7 - Website and eCommerce Builder for WordPress theme for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' attribute within the plugin's	2024-06-25	6.4	CVE-2024-5451

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
eCommerce Builder for WordPress	Icon and Heading widgets in all versions up to, and including, 11.13.0 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.			
Enalean--tuleap	Tuleap is an Open Source Suite to improve management of software developments and collaboration. Users are able to see backlog items that they should not see. This issue has been patched in Tuleap Community Edition version 15.9.99.97.	2024-06-25	4.3	CVE-2024-37167
ericsson -- codechecker	CodeChecker is an analyzer tooling, defect database and viewer extension for the Clang Static Analyzer and Clang Tidy. Zip files uploaded to the server endpoint of `CodeChecker store` are not properly sanitized. An attacker, using a path traversal attack, can load and display files on the machine of `CodeChecker server`. The vulnerable endpoint is `/Default/v6.53/CodeCheckerService@massStoreRun`. The path traversal vulnerability allows reading data on the machine of the `CodeChecker server`, with the same permission level as the `CodeChecker server`. The attack requires a user account on the `CodeChecker server`, with permission to store to a server, and view the stored report. This vulnerability has been patched in version 6.23.	2024-06-24	6.5	CVE-2023-49793
everthemess--Goya	The Goya theme for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'attra-color', 'attra-size', and 'product-cata' parameters in versions up to, and including, 1.0.8.7 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.	2024-06-29	6.1	CVE-2023-4017
fastly--js-compute-runtime	@fastly/js-compute is a JavaScript SDK and runtime for building Fastly Compute applications. The implementation of several functions were determined to include a use-after-free bug. This bug could allow for unintended data loss if the result of the preceding functions were sent anywhere else, and often results in a guest trap causing services to return a 500. This bug has been fixed in version 3.16.0 of the `@fastly/js-compute` package.	2024-06-26	5.3	CVE-2024-38375
finesoft_project -- finesoft	Cross Site Scripting vulnerability in Hangzhou Meisoft Information Technology Co., Ltd. Finesoft v.8.0 and before allows a remote attacker to execute arbitrary code via a crafted script to the login.jsp parameter.	2024-06-24	6.1	CVE-2024-37679
finesoft_project -- finesoft	Hangzhou Meisoft Information Technology Co., Ltd. FineSoft <=8.0 is affected by Cross Site Scripting (XSS) which allows remote attackers to execute arbitrary code. Enter any account and password, click Login, the page will report an error, and a controllable parameter will appear at the URL:weburl.	2024-06-24	6.1	CVE-2024-37680
gallerycreator--Gallery Blocks with Lightbox. Image Gallery, (HTML5 video , YouTube, Vimeo) Video Gallery and Lightbox for native gallery	The Gallery Blocks with Lightbox. Image Gallery, (HTML5 video , YouTube, Vimeo) Video Gallery and Lightbox for native gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'galleryID' and 'className' parameters in all versions up to, and including, 3.2.1 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.	2024-06-28	6.4	CVE-2024-5424
Genexis--Tilgin Fiber Home Gateway HG1522	A vulnerability was found in Genexis Tilgin Fiber Home Gateway HG1522 CSx000-01_09_01_12. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /status/product_info/. The manipulation of the argument product_info leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The	2024-06-26	4.3	CVE-2024-6355

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	associated identifier of this vulnerability is VDB-269755. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
gitlab -- gitlab	An issue was discovered in GitLab CE/EE affecting all versions starting from 9.2 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, with the processing logic for generating link in dependency files can lead to a regular expression DoS attack on the server	2024-06-27	6.5	CVE-2024-1493
gitlab -- gitlab	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.7 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows private job artifacts can be accessed by any user.	2024-06-27	6.5	CVE-2024-3959
gitlab -- gitlab	Multiple Denial of Service (DoS) conditions has been discovered in GitLab CE/EE affecting all versions starting from 1.0 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1 which allowed an attacker to cause resource exhaustion via banzai pipeline.	2024-06-27	6.5	CVE-2024-4557
gitlab -- gitlab	An issue was discovered in GitLab CE/EE affecting all versions starting from 12.0 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows for an attacker to cause a denial of service using a crafted OpenAPI file.	2024-06-27	5.5	CVE-2024-1816
gitlab -- gitlab	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.9 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows merge request title to be visible publicly despite being set as project members only.	2024-06-27	5.3	CVE-2024-2191
gitlab -- gitlab	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.9 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, where a stored XSS vulnerability could be imported from a project with malicious commit notes.	2024-06-27	5.4	CVE-2024-4901
gitlab -- gitlab	An issue was discovered in GitLab EE affecting all versions starting from 16.0 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows an attacker to access issues and epics without having an SSO session using Duo Chat.	2024-06-27	4.3	CVE-2024-3115
gitlab -- gitlab	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.1 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows non-project member to promote key results to objectives.	2024-06-27	4.3	CVE-2024-4011
gitlab -- gitlab	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.10 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows a project maintainer can delete the merge request approval policy via graphQL.	2024-06-27	4.9	CVE-2024-5430
h5p -- h5p	The Interactive Content WordPress plugin before 1.15.8 does not validate uploads which could allow a Contributors and above to update malicious SVG files, leading to Stored Cross-Site Scripting issues	2024-06-27	5.4	CVE-2024-3111
hashicorp -- retryablehttp	go-retryablehttp prior to 0.7.7 did not sanitize urls when writing them to its log file. This could lead to go-retryablehttp writing sensitive HTTP basic auth credentials to its log file. This vulnerability, CVE-2024-6104, was fixed in go-retryablehttp 0.7.7.	2024-06-24	5.5	CVE-2024-6104 security@hashicorp.com
HCL Software-- Connections	HCL Connections is vulnerable to a cross-site scripting attack where an attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user which leads to executing malicious script code. This may let the attacker steal cookie-based authentication credentials and comprise user's account then launch other attacks.	2024-06-25	5.4	CVE-2024-30112

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Hitachi--Hitachi Storage Provider for VMware vCenter	Incorrect Default Permissions vulnerability in Hitachi Storage Provider for VMware vCenter allows local users to read and write specific files.This issue affects Hitachi Storage Provider for VMware vCenter: from 3.1.0 before 3.7.4.	2024-06-25	4.4	CVE-2024-22385 hirt@hitachi.co.jp
IBM--Cloud Pak for Security	IBM Cloud Pak for Security (CP4S) 1.10.0.0 through 1.10.11.0 and IBM QRadar Software Suite 1.10.12.0 through 1.10.21.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 233673.	2024-06-28	4	CVE-2022-38383
IBM--Cognos Analytics	IBM Cognos Analytics 11.2.0, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 12.0.0, 12.0.1, and 12.0.2 is potentially vulnerable to cross site scripting (XSS). A remote attacker could execute malicious commands due to improper validation of column headings in Cognos Assistant. IBM X-Force ID: 282780.	2024-06-28	5.4	CVE-2024-25041
IBM--Cognos Analytics	IBM Cognos Analytics 11.2.0, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 12.0.0, 12.0.1, and 12.0.2 is vulnerable to improper certificate validation when using the IBM Planning Analytics Data Source Connection. This could allow an attacker to spoof a trusted entity by interfering in the communication path between IBM Planning Analytics server and IBM Cognos Analytics server. IBM X-Force ID: 283364.	2024-06-28	5.9	CVE-2024-25053
IBM--MQ	IBM MQ Console 9.3 LTS and 9.3 CD could disclose could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 292765.	2024-06-28	6.5	CVE-2024-35155
IBM--MQ	IBM MQ 9.3 LTS and 9.3 CD could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 292766.	2024-06-28	6.5	CVE-2024-35156
IBM--MQ	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS and 9.3 CD, in certain configurations, is vulnerable to a denial of service attack caused by an error processing messages when an API Exit using MQBUFMH is used. IBM X-Force ID: 290259.	2024-06-28	5.9	CVE-2024-31919
IBM--MQ	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, and 9.3 CD is vulnerable to a denial of service attack caused by an error applying configuration changes. IBM X-Force ID: 290335.	2024-06-28	5.9	CVE-2024-35116
IBM--Security Access Manager Docker	IBM Security Access Manager Docker 10.0.0.0 through 10.0.7.1 could disclose sensitive information to a local user to do improper permission controls. IBM X-Force ID: 261195.	2024-06-27	6.2	CVE-2023-38368
IBM--Security Access Manager Docker	IBM Security Access Manager Docker 10.0.0.0 through 10.0.7.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 261198.	2024-06-27	5.9	CVE-2023-38371
IBM--Security Verify Access Docker	IBM Security Access Manager Docker 10.0.0.0 through 10.0.7.1 could allow a local user to possibly elevate their privileges due to sensitive configuration information being exposed. IBM X-Force ID: 292413.	2024-06-28	6.2	CVE-2024-35137
IBM--Security Verify Access Docker	IBM Security Access Manager Docker 10.0.0.0 through 10.0.7.1 could allow a local user to obtain sensitive information from the container due to incorrect default permissions. IBM X-Force ID: 292415.	2024-06-28	6.2	CVE-2024-35139
IBM--Security Verify Access	IBM Security Verify Access 10.0.0 through 10.0.7.1 could allow a local user to obtain sensitive information from trace logs. IBM X-Force ID: 252183.	2024-06-27	6.2	CVE-2023-30430

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--Security Verify Access	IBM Security Verify Access 10.0.0.0 through 10.0.7.1, under certain configurations, could allow an unauthenticated attacker to cause a denial of service due to asymmetric resource consumption. IBM X-Force ID: 287615.	2024-06-27	5.3	CVE-2024-31883
IBM--Sterling B2B Integrator Standard Edition	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.2.0.2 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user 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: 265511.	2024-06-27	5.4	CVE-2023-42014
IBM--Sterling B2B Integrator Standard Edition	IBM Sterling B2B Integrator Standard Edition 6.1 and 6.2 does not restrict or incorrectly restricts frame objects or UI layers that belong to another application or domain, which can lead to user confusion about which interface the user is interacting with. IBM X-Force ID: 265508.	2024-06-27	4.3	CVE-2023-42011
IBM--Storage Defender - Resiliency Service	IBM Storage Defender - Resiliency Service 2.0.0 through 2.0.4 uses an inadequate account lockout setting that could allow an attacker on the network to brute force account credentials. IBM X-Force ID: 281678.	2024-06-28	6.5	CVE-2024-25031
IBM--Storage Defender - Resiliency Service	IBM Storage Defender - Resiliency Service 2.0.0 through 2.0.4 agent username and password error response discrepancy exposes product to brute force enumeration. IBM X-Force ID: 294869.	2024-06-28	5.3	CVE-2024-38322
IBM--WebSphere Application Server	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to cross-site scripting. This vulnerability allows a privileged user 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: 292640.	2024-06-27	4.8	CVE-2024-35153
itsourcecode--Tailoring Management System	A vulnerability, which was classified as critical, was found in itsourcecode Tailoring Management System 1.0. This affects an unknown part of the file customeradd.php. The manipulation of the argument fullname/address/phonenumber/sex/email/city/comment 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-269805 was assigned to this vulnerability.	2024-06-27	6.3	CVE-2024-6372
kadencewp -- gutenberg_blocks_with_ai	The Gutenberg Blocks with AI by Kadence WP - Page Builder Features plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Google Maps widget parameters in all versions up to, and including, 3.2.42 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.	2024-06-27	5.4	CVE-2024-5289
kadencewp -- kadence_blocks_pro	The kadence-blocks-pro WordPress plugin before 2.3.8 does not prevent users with at least the contributor role using some of its shortcode's functionalities to leak arbitrary options from the database.	2024-06-27	4.3	CVE-2024-1330
lahirudanushka--School Management System	A vulnerability was found in lahirudanushka School Management System 1.0.0/1.0.1 and classified as critical. Affected by this issue is some unknown functionality of the file examresults-par.php of the component Exam Results Page. The manipulation of the argument sid 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-269492.	2024-06-24	6.3	CVE-2024-6279
lahirudanushka--School Management	A vulnerability classified as critical has been found in lahirudanushka School Management System 1.0.0/1.0.1. This affects an unknown part of the file /attendancelist.php of the component Attendance Report Page. The manipulation of the argument aid leads to sql injection. It is possible to initiate the attack	2024-06-24	4.7	CVE-2024-6274

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
System	remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-269487.			
lahirudanushka--School Management System	A vulnerability classified as critical was found in lahirudanushka School Management System 1.0.0/1.0.1. This vulnerability affects unknown code of the file parent.php of the component Parent Page. The manipulation of the argument update 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-269488.	2024-06-24	4.7	CVE-2024-6275
lahirudanushka--School Management System	A vulnerability, which was classified as critical, has been found in lahirudanushka School Management System 1.0.0/1.0.1. This issue affects some unknown processing of the file teacher.php of the component Teacher Page. The manipulation of the argument update leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-269489 was assigned to this vulnerability.	2024-06-24	4.7	CVE-2024-6276
lahirudanushka--School Management System	A vulnerability, which was classified as critical, was found in lahirudanushka School Management System 1.0.0/1.0.1. Affected is an unknown function of the file student.php of the component Student Page. The manipulation of the argument update 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-269490 is the identifier assigned to this vulnerability.	2024-06-24	4.7	CVE-2024-6277
lahirudanushka--School Management System	A vulnerability has been found in lahirudanushka School Management System 1.0.0/1.0.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file subject.php of the component Subject Page. The manipulation of the argument update 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-269491.	2024-06-24	4.7	CVE-2024-6278
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: um: Add winch to winch_handlers before registering winch IRQ Registering a winch IRQ is racy, an interrupt may occur before the winch is added to the winch_handlers list. If that happens, register_winch_irq() adds to that list a winch that is scheduled to be (or has already been) freed, causing a panic later in winch_cleanup(). Avoid the race by adding the winch to the winch_handlers list before registering the IRQ, and rolling back if um_request_irq() fails.	2024-06-24	5.5	CVE-2024-39292
looswebstudio--SEO SIMPLE PACK	The SEO SIMPLE PACK plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 3.2.1 via META description. This makes it possible for unauthenticated attackers to extract limited information about password protected posts.	2024-06-28	5.3	CVE-2024-2795
Magarsus Consultancy--SSO (Single Sign On)	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Magarsus Consultancy SSO (Single Sign On) allows Manipulating Hidden Fields.This issue affects SSO (Single Sign On): from 1.0 before 1.1.	2024-06-26	6.1	CVE-2024-4604
ManageEngine--OpManager	Zoho ManageEngine ITOM products versions from 128234 to 128248 are affected by the stored cross-site scripting vulnerability in the proxy server option.	2024-06-24	6.3	CVE-2024-36038 0fc0942c-577d-436f-ae8e-945763c79b02
matter-labs--era-compiler-vyper	ZKsync Era is a layer 2 rollup that uses zero-knowledge proofs to scale Ethereum. There is possible invalid stack access due to the addresses used to access the stack not properly being converted to cells. This issue has been patched in version 1.5.0.	2024-06-28	6.5	CVE-2024-38533

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mediavine -- create	The Create by Mediavine plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Schema Meta shortcode in all versions up to, and including, 1.9.7 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.	2024-06-27	5.4	CVE-2024-5601
mermaid-js--zenuml-core	ZenUML is JavaScript-based diagramming tool that requires no server, using Markdown-inspired text definitions and a renderer to create and modify sequence diagrams. Markdown-based comments in the ZenUML diagram syntax are susceptible to Cross-site Scripting (XSS). The comment feature allows the user to attach small notes for reference. This feature allows the user to enter in their comment in markdown comment, allowing them to use common markdown features, such as `**` for bolded text. However, the markdown text is currently not sanitized before rendering, allowing an attacker to enter a malicious payload for the comment which leads to XSS. This puts existing applications that use ZenUML unsandboxed at risk of arbitrary JavaScript execution when rendering user-controlled diagrams. This vulnerability was patched in version 3.23.25,	2024-06-26	5.4	CVE-2024-38527
Mia Technology Inc.--Mia-Med Health Aplication	Use of a Broken or Risky Cryptographic Algorithm vulnerability in Mia Technology Inc. Mia-Med Health Aplication allows Signature Spoofing by Improper Validation.This issue affects Mia-Med Health Aplication: before 1.0.14.	2024-06-24	5.3	CVE-2024-3264
Moxa--OnCell G3150A-LTE Series	OnCell G3470A-LTE Series firmware versions v1.7.7 and prior have been identified as vulnerable due to accepting a format string from an external source as an argument. An attacker could modify an externally controlled format string to cause a memory leak and denial of service.	2024-06-25	6.3	CVE-2024-4641 psirt@moxa.com
n/a--djangorestframework	Versions of the package djangorestframework before 3.15.2 are vulnerable to Cross-site Scripting (XSS) via the break_long_headers template filter due to improper input sanitization before splitting and joining with tags.	2024-06-26	6.1	CVE-2024-21520
n/a--ESXi	VMware ESXi contains an out-of-bounds read vulnerability. A malicious actor with local administrative privileges on a virtual machine with an existing snapshot may trigger an out-of-bounds read leading to a denial-of-service condition of the host.	2024-06-25	6.8	CVE-2024-37086
n/a--vCenter Server	The vCenter Server contains a denial-of-service vulnerability. A malicious actor with network access to vCenter Server may create a denial-of-service condition.	2024-06-25	5.3	CVE-2024-37087
N/A--VMware Cloud Director Object Storage Extension	VMware Cloud Director Object Storage Extension contains an Insertion of Sensitive Information vulnerability. A malicious actor with adjacent access to web/proxy server logging may be able to obtain sensitive information from URLs that are logged.	2024-06-27	5.3	CVE-2024-22276
N/A--VMware Cloud Director	VMware Cloud Director contains an Improper Privilege Management vulnerability. An authenticated tenant administrator for a given organization within VMware Cloud Director may be able to accidentally disable their organization leading to a Denial of Service for active sessions within their own organization's scope.	2024-06-27	4.9	CVE-2024-22272
n/a--VMware ESXi	VMware ESXi contains an authentication bypass vulnerability. A malicious actor with sufficient Active Directory (AD) permissions can gain full access to an ESXi host that was previously configured to use AD for user management https://blogs.vmware.com/vsphere/2012/09/joining-vsphere-hosts-to-active-directory.html by re-creating the configured AD group ('ESXi Admins' by default) after it was deleted from AD.	2024-06-25	6.8	CVE-2024-37085

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
N/A--VMware Workspace One UEM	VMware Workspace One UEM update addresses an information exposure vulnerability. A malicious actor with network access to the Workspace One UEM may be able to perform an attack resulting in an information exposure.	2024-06-27	6.8	CVE-2024-22260
nattywp--Silesia	The Silesia theme for WordPress is vulnerable to Stored Cross-Site Scripting via the 'link' attribute within the theme's Button shortcode in all versions up to, and including, 1.0.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-28	6.4	CVE-2024-5788
netweblogic--Events Manager Calendar, Bookings, Tickets, and more!	The Events Manager - Calendar, Bookings, Tickets, and more! plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'country' parameter in all versions up to, and including, 6.4.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-06-29	6.1	CVE-2024-5889
Next4Biz CRM & BPM Software--Business Process Manangement (BPM)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Next4Biz CRM & BPM Software Business Process Manangement (BPM) allows Stored XSS.This issue affects Business Process Manangement (BPM): from 6.6.4.4 before 6.6.4.5.	2024-06-24	5.4	CVE-2024-4754
ninjateam -- wp_chat_app	The WP Chat App WordPress plugin before 3.6.5 does not sanitise and escape some of its settings, which could allow high privilege users such as admins to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed.	2024-06-27	4.8	CVE-2024-4664
petesheppard84--Extensions for Elementor	The Extensions for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter within the EE Button widget in all versions up to, and including, 2.0.30 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.	2024-06-29	6.4	CVE-2024-5666
Play.ht--Play.ht	Improper Authentication vulnerability in Play.Ht allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Play.Ht: from n/a through 3.6.4.	2024-06-24	4.3	CVE-2024-37233
posimythemes--The Plus Addons for Elementor Elementor Addons, Page Templates, Widgets, Mega Menu, WooCommerce	The The Plus Addons for Elementor - Elementor Addons, Page Templates, Widgets, Mega Menu, WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'video_color' parameter in all versions up to, and including, 5.6.0 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.	2024-06-27	6.4	CVE-2024-4983
Progress Software Corporation--WhatsUp Gold	In WhatsUp Gold versions released before 2023.1.3, a path traversal vulnerability exists. A specially crafted unauthenticated HTTP request to AppProfileImport can lead can lead to information disclosure.	2024-06-25	6.5	CVE-2024-5017
Progress Software Corporation--WhatsUp Gold	In WhatsUp Gold versions released before 2023.1.3, an unauthenticated Path Traversal vulnerability exists Wug.UI.Areas.Wug.Controllers.SessionController.LoadNMScript. This allows allows reading of any file from the applications web-root directory .	2024-06-25	5.3	CVE-2024-5018
Progress Software Corporation--	In WhatsUp Gold versions released before 2023.1.3, an unauthenticated Arbitrary File Read issue exists in	2024-06-25	5.3	CVE-2024-5019

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WhatsUp Gold	Wug.UI.Areas.Wug.Controllers.SessionController.CachedCSS. This vulnerability allows reading of any file with iisapppool\NmConsole privileges.			
ravichandra--Infinite	The Infinite theme for WordPress is vulnerable to Stored Cross-Site Scripting via the 'project_url' parameter in all versions up to, and including, 1.1.2 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.	2024-06-28	6.4	CVE-2024-5796
renesas -- rcar_gen3	Integer Underflow (Wrap or Wraparound) vulnerability in Renesas arm-trusted-firmware. An integer underflow in image range check calculations could lead to bypassing address restrictions and loading of images to unallowed addresses.	2024-06-24	6.7	CVE-2024-6285
rocklobster -- contact_form_7	The Contact Form 7 WordPress plugin before 5.9.5 has an open redirect that allows an attacker to utilize a false URL and redirect to the URL of their choosing.	2024-06-27	6.1	CVE-2024-4704
scidsg--hushline	Hush Line is a free and open-source, anonymous-tip-line-as-a-service for organizations or individuals. The CSP policy applied on the `tips.hushline.app` website and bundled by default in this repository is trivial to bypass. This vulnerability has been patched in version 0.1.0.	2024-06-28	6.3	CVE-2024-38522
silabs.com--SiSDK	In a Silicon Labs multi-protocol gateway, a corrupt pointer to buffered data on a multi-protocol radio co-processor (RCP) causes the OpenThread Border Router(OTBR) application task running on the host platform to crash, allowing an attacker to cause a temporary denial-of-service.	2024-06-27	6.5	CVE-2024-3017
SourceCodester--Simple Online Bidding System	A vulnerability was found in SourceCodester Simple Online Bidding System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/ajax.php?action=save_settings. The manipulation of the argument img 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 identifier VDB-269493 was assigned to this vulnerability.	2024-06-24	6.3	CVE-2024-6280
Spotfire--Spotfire Enterprise Runtime for R - Server Edition	Vulnerability in Spotfire Spotfire Enterprise Runtime for R - Server Edition, Spotfire Spotfire Statistics Services, Spotfire Spotfire Analyst, Spotfire Spotfire Desktop, Spotfire Spotfire Server allows The impact of this vulnerability depends on the privileges of the user running the affected software..This issue affects Spotfire Enterprise Runtime for R - Server Edition: from 1.12.7 through 1.20.0; Spotfire Statistics Services: from 12.0.7 through 12.3.1, from 14.0.0 through 14.3.0; Spotfire Analyst: from 12.0.9 through 12.5.0, from 14.0.0 through 14.3.0; Spotfire Desktop: from 14.0 through 14.3.0; Spotfire Server: from 12.0.10 through 12.5.0, from 14.0.0 through 14.3.0.	2024-06-27	6.8	CVE-2024-3331 security@tibco.com
squid-cache--squid	Squid is a caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. Due to an Out-of-bounds Write error when assigning ESI variables, Squid is susceptible to a Memory Corruption error. This error can lead to a Denial of Service attack.	2024-06-25	6.3	CVE-2024-37894
Synology--Camera Firmware	A vulnerability regarding improper limitation of a pathname to a restricted directory ('Path Traversal') is found in the Language Settings functionality. This allows remote attackers to read specific files containing non-sensitive information via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.7-0298 may be affected: BC500 and TC500.	2024-06-28	5.3	CVE-2023-47803
Synology--Camera Firmware	A vulnerability regarding incorrect authorization is found in the firmware upgrade functionality. This allows remote authenticated users with administrator privileges to bypass firmware integrity check via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.7-0298 may be affected: BC500 and TC500.	2024-06-28	4.9	CVE-2024-39352

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Synology--Synology Router Manager (SRM)	Incorrect default permissions vulnerability in firewall functionality in Synology Router Manager (SRM) before 1.2.5-8227-11 and 1.3.1-9346-8 allows man-in-the-middle attackers to access highly sensitive intranet resources via unspecified vectors.	2024-06-28	5.9	CVE-2024-39347
Talya Informatics--Travel APPS	Improper Access Control vulnerability in Talya Informatics Travel APPS allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Travel APPS: before v17.0.68.	2024-06-27	4.3	CVE-2024-1153
tatvic--Conversios Google Analytics 4 (GA4), Google Ads, Meta Pixel & more for WooCommerce	The Conversios - Google Analytics 4 (GA4), Meta Pixel & more Via Google Tag Manager For WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tiktok_user_id' parameter in all versions up to, and including, 7.0.12 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.	2024-06-28	4.7	CVE-2024-6288
Tenda--A301	A vulnerability classified as critical was found in Tenda A301 15.13.08.12. Affected by this vulnerability is the function fromSetWirelessRepeat of the file /goform/SetOnlineDevName. The manipulation of the argument devName leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-269947. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-28	6.5	CVE-2024-6402
Tenda--A301	A vulnerability, which was classified as critical, has been found in Tenda A301 15.13.08.12. Affected by this issue is the function formWifiBasicSet of the file /goform/SetOnlineDevName. The manipulation of the argument devName leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-269948. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-28	6.5	CVE-2024-6403
The Conduit Contributors--Conduit	Lack of validation of origin in federation API in Conduit, allowing any remote server to impersonate any user from any server in most EDUs	2024-06-25	5.3	CVE-2024-6301
The Conduit Contributors--Conduit	Lack of consideration of key expiry when validating signatures in Conduit, allowing an attacker which has compromised an expired key to forge requests as the remote server, as well as PDUs with timestamps past the expiry date	2024-06-25	4.8	CVE-2024-6299
thehappymonster--Happy Addons for Elementor	The Happy Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' attribute within the plugin's Gradient Heading widget in all versions up to, and including, 3.11.1 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.	2024-06-29	6.4	CVE-2024-5790
timstrifler--Exclusive Addons for Elementor	The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Card widget in all versions up to, and including, 2.6.9.8 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.	2024-06-26	6.4	CVE-2024-5332
tislam100--Scylla lite	The Scylla lite theme for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter within the theme's Button shortcode in all versions up to, and including, 1.8.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and	2024-06-28	6.4	CVE-2024-5922

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
tislam100--Theron Lite	The Theron Lite theme for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter within the theme's Button shortcode in all versions up to, and including, 2.0 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.	2024-06-28	6.4	CVE-2024-5925
tpm2-software--tpm2-tools	tpm2-tools is the source repository for the Trusted Platform Module (TPM2.0) tools. A malicious attacker can generate arbitrary quote data which is not detected by `tpm2 checkquote`. This issue was patched in version 5.7.	2024-06-28	4.3	CVE-2024-29038
tpm2-software--tpm2-tss	This repository hosts source code implementing the Trusted Computing Group's (TCG) TPM2 Software Stack (TSS). The JSON Quote Info returned by Fapi_Quote has to be deserialized by Fapi_VerifyQuote to the TPM Structure `TPMS_ATTEST`. For the field `TPM2_GENERATED magic` of this structure any number can be used in the JSON structure. The verifier can receive a state which does not represent the actual, possibly malicious state of the device under test. The malicious device might get access to data it shouldn't, or can use services it shouldn't be able to. This issue has been patched in version 4.1.0.	2024-06-28	4.3	CVE-2024-29040
trudesk_project --trudesk	TruDesk Help Desk/Ticketing Solution v1.1.11 is vulnerable to a Cross-Site Request Forgery (CSRF) attack which would allow an attacker to restart the server, causing a DoS attack. The attacker must craft a webpage that would perform a GET request to the /api/v1/admin/restart endpoint, then the victim (who has sufficient privileges), would visit the page and the server restart would begin. The attacker must know the full URL that TruDesk is on in order to craft the webpage.	2024-06-24	6.5	CVE-2021-45785
twinpictures, baden03--jQuery T(-) Countdown Widget	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in twinpictures, baden03 jQuery T(-) Countdown Widget allows Stored XSS.This issue affects jQuery T(-) Countdown Widget: from n/a through 2.3.25.	2024-06-26	6.5	CVE-2024-37247
urkekg--Stock Ticker	The Stock Ticker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's stock_ticker shortcode in all versions up to, and including, 3.24.4 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.	2024-06-29	6.4	CVE-2024-6363
virtosoftware --sharepoint_bulk_file_download	An issue was discovered in VirtoSoftware Virto Bulk File Download 5.5.44 for SharePoint 2019. It discloses full pathnames via Virto.SharePoint.FileDownloader/Api/Download.ashx?action=archive.	2024-06-24	5.3	CVE-2024-33880
virtosoftware --sharepoint_bulk_file_download	An issue was discovered in VirtoSoftware Virto Bulk File Download 5.5.44 for SharePoint 2019. The Virto.SharePoint.FileDownloader/Api/Download.ashx isCompleted method allows an NTLMv2 hash leak via a UNC share pathname in the path parameter.	2024-06-24	5.3	CVE-2024-33881
VMware--Salt Project	Syndic cache directory creation is vulnerable to a directory traversal attack in salt project which can lead a malicious attacker to create an arbitrary directory on a Salt master.	2024-06-27	5	CVE-2024-22231
webtechstreet --elementor_addon_elements	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter in versions up to, and including, 1.13.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject	2024-06-27	5.4	CVE-2024-4569

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.			
webtechstreet -- elementor_addon_elements	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter in versions up to, and including, 1.13.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-06-27	5.4	CVE-2024-4570
WordPress Foundation--WordPress	WordPress Core is vulnerable to Stored Cross-Site Scripting via the HTML API in various versions prior to 6.5.5 due to insufficient input sanitization and output escaping on URLs. 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.	2024-06-25	6.4	CVE-2024-6307
wpzita--Zita Elementor Site Library	The Zita Elementor Site Library plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the import_xml_data, xml_data_import, import_option_data, import_widgets, and import_customizer_settings functions in all versions up to, and including, 1.6.2. This makes it possible for authenticated attackers, with subscriber-level access and above, to create pages, update certain options, including WooCommerce page titles and Elementor settings, import widgets, and update the plugin's customizer settings and the WordPress custom CSS. NOTE: This vulnerability was partially fixed in version 1.6.2.	2024-06-25	4.3	CVE-2024-3249
xwiki -- xwiki	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The content of a document included using `{{include reference="targetdocument"/}}` is executed with the right of the includer and not with the right of its author. This means that any user able to modify the target document can impersonate the author of the content which used the `include` macro. This vulnerability has been patched in XWiki 15.0 RC1 by making the default behavior safe.	2024-06-24	4.3	CVE-2024-38369
Yokogawa Electric Corporation--FAST/TOOLS	A vulnerability has been found in FAST/TOOLS and CI Server. The affected product's WEB HMI server's function to process HTTP requests has a security flaw (Reflected XSS) that allows the execution of malicious scripts. Therefore, if a client PC with inadequate security measures accesses a product URL containing a malicious request, the malicious script may be executed on the client PC. The affected products and versions are as follows: FAST/TOOLS (Packages: RVSVRN, UNSVRN, HMIWEB, FTEES, HMIMOB) R9.01 to R10.04 CI Server R1.01.00 to R1.03.00	2024-06-26	5.8	CVE-2024-4105
Yokogawa Electric Corporation--FAST/TOOLS	A vulnerability has been found in FAST/TOOLS and CI Server. The affected products have built-in accounts with no passwords set. Therefore, if the product is operated without a password set by default, an attacker can break into the affected product. The affected products and versions are as follows: FAST/TOOLS (Packages: RVSVRN, UNSVRN, HMIWEB, FTEES, HMIMOB) R9.01 to R10.04 CI Server R1.01.00 to R1.03.00	2024-06-26	5.3	CVE-2024-4106

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
All In One WP Security & Firewall Team--All In One	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in All In One WP Security & Firewall Team All In One WP Security & Firewall allows	2024-06-04	3.7	CVE-2023-52147

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WP Security & Firewall	Accessing Functionality Not Properly Constrained by ACLs.This issue affects All In One WP Security & Firewall: from n/a through 5.2.4.			
Born05--CraftCMS Plugin - Two-Factor Authentication	The CraftCMS plugin Two-Factor Authentication in versions 3.3.1, 3.3.2 and 3.3.3 discloses the password hash of the currently authenticated user after submitting a valid TOTP.	2024-06-06	3.7	CVE-2024-5657
David Vongries--Ultimate Dashboard	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in David Vongries Ultimate Dashboard allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Ultimate Dashboard: from n/a through 3.7.10.	2024-06-04	3.7	CVE-2023-49822
Event Espresso--Event Espresso 4 Decaf	Missing Authorization vulnerability in Event Espresso Event Espresso 4 Decaf allows Functionality Misuse.This issue affects Event Espresso 4 Decaf: from n/a through 4.10.44.Decaf.	2024-06-03	3.7	CVE-2023-27437
evmos--evmos	Evmos is the Ethereum Virtual Machine (EVM) Hub on the Cosmos Network. The spendable balance is not updated properly when delegating vested tokens. The issue allows a clawback vesting account to anticipate the release of unvested tokens. This vulnerability is fixed in 18.0.0.	2024-06-06	3.5	CVE-2024-32873
Florent Maillefaud--WP Maintenance	Authentication Bypass by Spoofing vulnerability in WP Maintenance allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects WP Maintenance: from n/a through 6.1.3.	2024-06-04	3.7	CVE-2023-47769
LWS--LWS Hide Login	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in LWS LWS Hide Login allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects LWS Hide Login: from n/a through 2.1.8.	2024-06-04	3.7	CVE-2023-47818
n/a--Likeshop	A vulnerability was found in Likeshop up to 2.5.7 and classified as problematic. This issue affects some unknown processing of the file /admin of the component Merchandise Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The identifier VDB-267449 was assigned to this vulnerability.	2024-06-08	2.4	CVE-2024-5766
n/a--n/a	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service.	2024-06-05	3.7	CVE-2023-50803
n/a--n/a	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check format types specified by the NAS (Non-Access-Stratum) module. This can lead to bypass of authentication.	2024-06-05	3.7	CVE-2023-50804
Webcraftic--Hide login page	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Webcraftic Hide login page allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Hide login page: from n/a through 1.1.9.	2024-06-04	3.7	CVE-2023-48335
WpDevArt--Booking calendar, Appointment Booking System	External Control of Assumed-Immutable Web Parameter vulnerability in WpDevArt Booking calendar, Appointment Booking System allows Manipulating Hidden Fields.This issue affects Booking calendar, Appointment Booking System: from n/a through 3.2.3.	2024-06-03	3.7	CVE-2023-24373
wpdevart--Coming soon and Maintenance	Authentication Bypass by Spoofing vulnerability in wpdevart Coming soon and Maintenance mode allows Accessing Functionality Not Properly Constrained by	2024-06-04	3.7	CVE-2023-49741

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mode	ACLs.This issue affects Coming soon and Maintenance mode: from n/a through 3.7.3.			
WPServeur, NicolasKulka, wpformation--WPS Hide Login	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in WPServeur, NicolasKulka, wpformation WPS Hide Login allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects WPS Hide Login: from n/a through 1.9.11.	2024-06-04	3.7	CVE-2023-49748
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by an Improper Input Validation vulnerability that could result in a security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect the integrity of the page. Exploitation of this issue requires user interaction.	2024-06-13	3.5	CVE-2024-26126
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by an Improper Input Validation vulnerability that could result in a security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect the integrity of the page. Exploitation of this issue requires user interaction.	2024-06-13	3.5	CVE-2024-26127
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by an Improper Input Validation vulnerability that could result in a security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect the integrity of the page. Exploitation of this issue requires user interaction.	2024-06-13	3.5	CVE-2024-36226
BeyondTrust--BeyondInsight PasswordSafe	A low severity vulnerability in BIPS has been identified where an attacker with high privileges or a compromised high privilege account can overwrite Read-Only smart rules via a specially crafted API request.	2024-06-11	3.3	CVE-2024-5812
Fortinet--FortiProxy	A use of password hash with insufficient computational effort vulnerability [CWE-916] affecting FortiOS version 7.4.3 and below, 7.2 all versions, 7.0 all versions, 6.4 all versions and FortiProxy version 7.4.2 and below, 7.2 all versions, 7.0 all versions, 2.0 all versions may allow aÂ privileged attacker with super-admin profile and CLI access to decrypting the backup file.	2024-06-11	1.8	CVE-2024-21754
GitLab--GitLab	DoS in KAS in GitLab CE/EE affecting all versions from 16.10.0 prior to 16.10.6 and 16.11.0 prior to 16.11.3 allows an attacker to crash KAS via crafted gRPC requests.	2024-06-14	3.1	CVE-2024-5469
Harbor--Harbor	SQL-Injection in Harbor allows priviledge users to leak the task IDs	2024-06-11	2.7	CVE-2024-22261
HashiCorp--Vault	Vault and Vault Enterprise did not properly validate the JSON Web Token (JWT) role-bound audience claim when using the Vault JWT auth method. This may have resulted in Vault validating a JWT the audience and role-bound claims do not match, allowing an invalid login to succeed when it should have been rejected. This vulnerability, CVE-2024-5798, was fixed in Vault and Vault Enterprise 1.17.0, 1.16.3, and 1.15.9	2024-06-12	2.6	CVE-2024-5798 security@hashicorp.com
HCL Software--DRYiCE Optibot Reset Station	HCL DRYiCE Optibot Reset StationÂ is impacted by a missing Strict Transport Security Header. Â This could allow an attacker to intercept or manipulate data during redirection.	2024-06-14	3.7	CVE-2024-30119
HCL Software--DRYiCE Optibot Reset Station	HCL DRYiCE Optibot Reset Station is impacted by an Unused Parameter in the web application.	2024-06-14	2.9	CVE-2024-30120

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Hitachi Energy--FOXMAN-UN	A vulnerability exists in the FOXMAN-UN/UNEM in which sensitive information is stored in cleartext within a resource that might be accessible to another control sphere.	2024-06-11	1.9	CVE-2024-28024
IBM--i	IBM Db2 for i 7.2, 7.3, 7.4, and 7.5 supplies user defined table function is vulnerable to user enumeration by a local authenticated attacker, without having authority to the related *USRPRF objects. This can be used by a malicious actor to gather information about users that can be targeted in further attacks. IBM X-Force ID: 287174.	2024-06-15	3.3	CVE-2024-31870
Mattermost--Mattermost	Mattermost Desktop App versions <=5.7.0 fail to disable certain Electron debug flags which allows for bypassingÂ TCC restrictions on macOS.	2024-06-14	3.8	CVE-2024-36287
n/a--playSMS	A vulnerability classified as problematic has been found in playSMS up to 1.4.7. Affected is an unknown function of the file /index.php?app=main&inc=feature_schedule&op=list of the component SMS Schedule Handler. The manipulation of the argument name/message leads to basic cross site scripting. It is possible to launch the attack remotely. Upgrading to version 1.4.8 is able to address this issue. The name of the patch is 7a88920f6b536c6a91512e739bcb4e8adefeed2b. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-267912. NOTE: The code maintainer was contacted early about this disclosure and was eager to prepare a fix as quickly as possible.	2024-06-11	3.5	CVE-2024-5851
nextcloud--security-advisories	Nextcloud Photos is a photo management app. Users can remove photos from the album of registered users. It is recommended that the Nextcloud Server is upgraded to 25.0.7 or 26.0.2 and the Nextcloud Enterprise Server is upgraded to 25.0.7 or 26.0.2.	2024-06-14	3.5	CVE-2024-37314
nextcloud--security-advisories	Nextcloud Server is a self hosted personal cloud system. An attacker with read-only access to a file is able to restore older versions of a document when the files_versions app is enabled. It is recommended that the Nextcloud Server is upgraded to 26.0.12, 27.1.7 or 28.0.3 and that the Nextcloud Enterprise Server is upgraded to 23.0.12.16, 24.0.12.12, 25.0.13.6, 26.0.12, 27.1.7 or 28.0.3.	2024-06-14	3.5	CVE-2024-37315
nextcloud--security-advisories	Nextcloud Server is a self hosted personal cloud system. A malicious user was able to send delete requests for old versions of files they only got shared with read permissions. It is recommended that the Nextcloud Server is upgraded to 26.0.12 or 27.1.7 or 28.0.3 and that the Nextcloud Enterprise Server is upgraded to 26.0.12 or 27.1.7 or 28.0.3.	2024-06-14	3.5	CVE-2024-37884
nextcloud--security-advisories	The Nextcloud Desktop Client is a tool to synchronize files from Nextcloud Server with your computer. A code injection in Nextcloud Desktop Client for macOS allowed to load arbitrary code when starting the client with DYLD_INSERT_LIBRARIES set in the enviroment. It is recommended that the Nextcloud Desktop client is upgraded to 3.12.0.	2024-06-14	3.8	CVE-2024-37885
nextcloud--security-advisories	Nextcloud Server is a self hosted personal cloud system. Private shared calendar events' recurrence exceptions can be read by sharees. It is recommended that the Nextcloud Server is upgraded to 27.1.10 or 28.0.6 or 29.0.1 and that the Nextcloud Enterprise Server is upgraded to 27.1.10 or 28.0.6 or 29.0.1.	2024-06-14	3.5	CVE-2024-37887
Red Hat--Red Hat Build of Keycloak	A Cross-site request forgery (CSRF) flaw was found in Keycloak and occurs due to the lack of a unique token sent during the authentication POST request, /login-actions/authenticate. This flaw allows an attacker to craft a malicious login page and trick a legitimate user of an application into authenticating with an attacker-controlled account instead of their own.	2024-06-12	3.7	CVE-2024-5203
SAP_SE--SAP BusinessObjects Business	On Unix, SAP BusinessObjects Business Intelligence Platform (Scheduling) allows an authenticated attacker with administrator access on the local server to access the	2024-06-11	3.7	CVE-2024-34684

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Intelligence Platform	password of a local account. As a result, an attacker can obtain non-administrative user credentials, which will allow them to read or modify the remote server files.			
Siemens--TIA Administrator	A vulnerability has been identified in TIA Administrator (All versions < V3 SP2). The affected component creates temporary download files in a directory with insecure permissions. This could allow any authenticated attacker on Windows to disrupt the update process.	2024-06-11	3.3	CVE-2023-38533
smallweigit--Avue	A vulnerability classified as problematic was found in smallweigit Avue up to 3.4.4. Affected by this vulnerability is an unknown functionality of the component avueUeditor. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-267895. NOTE: The code maintainer explains, that "rich text is no longer maintained".	2024-06-11	3.5	CVE-2024-5829
smub--Easy WP SMTP by SendLayer WordPress SMTP and Email Log Plugin	The Easy WP SMTP by SendLayer - WordPress SMTP and Email Log Plugin plugin for WordPress is vulnerable to information exposure in all versions up to, and including, 2.3.0. This is due to plugin providing the SMTP password in the SMTP Password field when viewing the settings. This makes it possible for authenticated attackers, with administrative-level access and above, to view the SMTP password for the supplied server. Although this would not be useful for attackers in most cases, if an administrator account becomes compromised this could be useful information to an attacker in a limited environment.	2024-06-13	2.7	CVE-2024-3073
strapi--strapi	Strapi is an open-source content management system. Prior to version 4.19.1, a super admin can create a collection where an item in the collection has an association to another collection. When this happens, another user with Author Role can see the list of associated items they did not create. They should see nothing but their own items they created not all items ever created. Users should upgrade @strapi/plugin-content-manager to version 4.19.1 to receive a patch.	2024-06-12	2.3	CVE-2024-29181
Tenable--Security Center	A stored cross site scripting vulnerability exists in Tenable Security Center where an authenticated, remote attacker could inject HTML code into a web application scan result page.	2024-06-12	3.5	CVE-2024-1891 vulnreport@tenable.com
ZKTeco--ZKBio CVSecurity V5000	A vulnerability was found in ZKTeco ZKBio CVSecurity V5000 4.1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Department Section. The manipulation of the argument Department Name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-268693 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-15	3.5	CVE-2024-6005
ZKTeco--ZKBio CVSecurity V5000	A vulnerability was found in ZKTeco ZKBio CVSecurity V5000 4.1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Summer Schedule Handler. The manipulation of the argument Schedule 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-268694 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-15	3.5	CVE-2024-6006
authzed--spicedb	Spicedb is an Open Source, Google Zanzibar-inspired permissions database to enable fine-grained authorization for customer applications. Use of an exclusion under an arrow that has multiple resources may resolve to `NO_PERMISSION` when permission is expected. If the resource exists under *multiple* folders and the user has access to view more than a single folder, SpiceDB may report the user does not have access due to a failure in the exclusion dispatcher to request that *all* the folders in which the user is a member be returned. Permission is returned as `NO_PERMISSION` when `PERMISSION` is expected on the `CheckPermission`	2024-06-20	3.7	CVE-2024-38361

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	API. This issue has been addressed in version 1.33.1. All users are advised to upgrade. There are no known workarounds for this issue.			
evmos--evmos	Evmos is the Ethereum Virtual Machine (EVM) Hub on the Cosmos Network. Preliminary checks on actions computed by the clawback vesting accounts are performed in the ante handler. Evmos core, implements two different ante handlers: one for Cosmos transactions and one for Ethereum transactions. Checks performed on the two implementation are different. The vulnerability discovered allowed a clawback account to bypass Cosmos ante handler checks by sending an Ethereum transaction targeting a precompile used to interact with a Cosmos SDK module. This vulnerability is fixed in 18.0.0.	2024-06-17	3.5	CVE-2024-37158
evmos--evmos	Evmos is the Ethereum Virtual Machine (EVM) Hub on the Cosmos Network. This vulnerability allowed a user to create a validator using vested tokens to deposit the self-bond. This vulnerability is fixed in 18.0.0.	2024-06-17	3.5	CVE-2024-37159
Ingenico--Estate Manager	A vulnerability, which was classified as problematic, has been found in Ingenico Estate Manager 2023. This issue affects some unknown processing of the file /emgui/rest/ums/messages of the component News Feed. The manipulation of the argument message 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-268787. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-17	2.4	CVE-2024-6059
JetBrains--Hub	In JetBrains Hub before 2024.2.34646 stored XSS via project description was possible	2024-06-18	3.5	CVE-2024-38507
LabVantage--LIMS	A vulnerability classified as problematic has been found in LabVantage LIMS 2017. This affects an unknown part of the file /labvantage/rc?command=page&page=SampleHistoricalList&_iframename=list&__crc=crc_1701669816260. The manipulation of the argument height/width 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-268785 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-17	3.5	CVE-2024-6058
LabVantage--LIMS	A vulnerability was found in LabVantage LIMS 2017. It has been declared as problematic. This vulnerability affects unknown code of the file /labvantage/rc?command=file&file=WEB-CORE/elements/files/filesembedded.jsp&size=32. The manipulation of the argument height/width 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-269152. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-20	3.5	CVE-2024-6181
LabVantage--LIMS	A vulnerability was found in LabVantage LIMS 2017. It has been rated as problematic. This issue affects some unknown processing of the file /labvantage/rc?command=page&page=LV_ViewSampleSpec&oosonly=Y&_sdialog=Y. The manipulation of the argument sdcid/keyid1 leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-269153 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-20	3.5	CVE-2024-6182
n/a--GPAC	A vulnerability has been found in GPAC 2.5-DEV-rev228-g11067ea92-master and classified as problematic. Affected by this vulnerability is the function isoffin_process of the file src/filters/isoffin_read.c of the component MP4Box. The manipulation leads to infinite loop. 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 the patch is 20c0f29139a82779b86453ce7f68d0681ec7624c. It is recommended	2024-06-17	3.3	CVE-2024-6061

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to apply a patch to fix this issue. The identifier VDB-268789 was assigned to this vulnerability.			
n/a--GPAC	A vulnerability was found in GPAC 2.5-DEV-rev228-g11067ea92-master and classified as problematic. Affected by this issue is the function swf_svg_add_iso_sample of the file src/filters/load_text.c of the component MP4Box. The manipulation leads to null pointer dereference. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The patch is identified as 31e499d310a48bd17c8b055a0bfe0fe35887a7cd. It is recommended to apply a patch to fix this issue. VDB-268790 is the identifier assigned to this vulnerability.	2024-06-17	3.3	CVE-2024-6062
n/a--GPAC	A vulnerability was found in GPAC 2.5-DEV-rev228-g11067ea92-master. It has been classified as problematic. This affects the function m2tsdmx_on_event of the file src/filters/dmx_m2ts.c of the component MP4Box. The manipulation leads to null pointer dereference. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The patch is named 8767ed0a77c4b02287db3723e92c2169f67c85d5. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-268791.	2024-06-17	3.3	CVE-2024-6063
n/a--PHPVibe	A vulnerability, which was classified as problematic, has been found in PHPVibe 11.0.46. This issue affects some unknown processing of the file functionalities.global.php of the component Global Options Page. The manipulation of the argument site-logo-text 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-268823. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-17	2.4	CVE-2024-6082
n/a--playSMS	A vulnerability, which was classified as problematic, was found in playSMS 1.4.3. Affected is an unknown function of the file /index.php?app=main&inc=feature_phonebook&op=phonebook_list of the component New Phonebook Handler. The manipulation of the argument name/email leads to basic cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-269418 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-22	2.4	CVE-2024-6251
n/a--spa-cartcms	A vulnerability, which was classified as problematic, was found in spa-cartcms 1.9.0.6. Affected is an unknown function of the file /login of the component Username Handler. The manipulation of the argument email leads to observable behavioral discrepancy. 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-268896.	2024-06-18	3.7	CVE-2024-6129
nasirkhan--Laravel Starter	A vulnerability was found in nasirkhan Laravel Starter up to 11.8.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /forgot-password of the component Password Reset Handler. The manipulation of the argument Email leads to observable response discrepancy. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-268784. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-17	3.7	CVE-2024-6056
Red Hat--Red Hat Build of Keycloak	A vulnerability was found in Keycloak. The LDAP testing endpoint allows changing the Connection URLÃ, independently without re-entering the currently configured LDAP bind credentials. This flaw allows an attacker with adminÃ, access (permission manage-realm) to change the LDAP host URL ("Connection URL") to a machine they control. The Keycloak server will connect to the attacker's host and try to authenticate with the configured credentials, thus leaking them to the attacker. As a consequence, an attacker who has compromised the admin console	2024-06-18	2.7	CVE-2024-5967

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	or compromised a user with sufficient privileges can leak domain credentials and attack the domain.			
SolidWP--Solid Security	Use of Less Trusted Source vulnerability in SolidWP Solid Security allows HTTP DoS.This issue affects Solid Security: from n/a through 9.3.1.	2024-06-21	3.7	CVE-2022-44593
SourceCodester--Simple Student Attendance System	A vulnerability was found in SourceCodester Simple Student Attendance System 1.0 and classified as problematic. Affected by this issue is the function get_student of the file student_form.php. The manipulation of the argument id 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-269276.	2024-06-21	3.5	CVE-2024-6212
wasmerio--wasmer	Wasmer is a web assembly (wasm) Runtime supporting WASIX, WASI and Emscripten. If the preopened directory has a symlink pointing outside, WASI programs can traverse the symlink and access host filesystem if the caller sets both `oflags::creat` and `rights::fd_write`. Programs can also crash the runtime by creating a symlink pointing outside with `path_symlink` and `path_open`ing the link. This issue has been addressed in commit `b9483d022` which has been included in release version 4.3.2. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-06-19	2.9	CVE-2024-38358
Zorlan--SkyCaiji	A vulnerability has been found in Zorlan SkyCaiji up to 2.8 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Task Handler. The manipulation of the argument onerror leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-269419.	2024-06-22	2.4	CVE-2024-6252
bigbluebutton--bigbluebutton	BigBlueButton is an open-source virtual classroom designed to help teachers teach and learners learn. An attacker may be able to exploit the overly elevated file permissions in the `/usr/local/bigbluebutton/core/vendor/bundle/ruby/2.7.0/gems/resque-2.6.0` directory with the goal of privilege escalation, potentially exposing sensitive information on the server. This issue has been patched in version(s) 2.6.18, 2.7.8 and 3.0.0-alpha.7.	2024-06-28	3.7	CVE-2024-39302
Checkmk GmbH--Checkmk	Insertion of Sensitive Information into Log File in Checkmk GmbH's Checkmk versions <2.3.0p7, <2.2.0p28, <2.1.0p45 and <=2.0.0p39 (EOL) causes automation user secrets to be written to audit log files accessible to administrators.	2024-06-26	2.7	CVE-2024-28830
Dell--CloudLink	Dell Key Trust Platform, v3.0.6 and prior, contains Use of a Cryptographic Primitive with a Risky Implementation vulnerability. A local privileged attacker could potentially exploit this vulnerability, leading to privileged information disclosure.	2024-06-28	3.8	CVE-2024-37137
Dell--CPG BIOS	Dell Client Platform BIOS contains an Out-of-bounds Write vulnerability in an externally developed component. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Information tampering.	2024-06-25	3.8	CVE-2024-32855
Dell--PowerProtect DD	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 contain an open redirect vulnerability. A remote low privileged attacker could potentially exploit this vulnerability, leading to information disclosure.	2024-06-26	3.5	CVE-2024-37141
Dell--PowerProtect DD	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 contain a disclosure of temporary sensitive information vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to the reuse of disclosed information to gain unauthorized access to the application report.	2024-06-26	2.7	CVE-2024-29177
DSpace--DSpace	DSpace is an open source software is a turnkey repository application used by more than 2,000 organizations and institutions worldwide to provide durable access to digital resources. In DSpace 7.0 through 7.6.1, when an HTML, XML or	2024-06-26	2.6	CVE-2024-38364

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	JavaScript Bitstream is downloaded, the user's browser may execute any embedded JavaScript. If that embedded JavaScript is malicious, there is a risk of an XSS attack. This vulnerability has been patched in version 7.6.2.			
HCL Software--Connections	HCL Connections contains a broken access control vulnerability that may allow unauthorized user to update data in certain scenarios.	2024-06-25	3.5	CVE-2023-37541
HCL Software--DRYiCE AEX	HCL DRYiCE AEX is impacted by a lack of clickjacking protection in the AEX web application. An attacker can use multiple transparent or opaque layers to trick a user into clicking on a button or link on another page than the one intended.	2024-06-28	3.7	CVE-2024-30109
HCL Software--DRYiCE AEX	HCL DRYiCE AEX product is impacted by lack of input validation vulnerability in a particular web application. A malicious script can be injected into a system which can cause the system to behave in unexpected ways.	2024-06-28	3.7	CVE-2024-30110
HCL Software--DRYiCE AEX	HCL DRYiCE AEX product is impacted by Missing Root Detection vulnerability in the mobile application. The mobile app can be installed in the rooted device due to which malicious users can gain unauthorized access to the rooted devices, compromising security and potentially leading to data breaches or other malicious activities.	2024-06-28	3.3	CVE-2024-30111
HCL Software--DRYiCE AEX	HCL DRYiCE AEX is potentially impacted by disclosure of sensitive information in the mobile application when a snapshot is taken.	2024-06-28	3.3	CVE-2024-30135
Kareadita--Kavita	Kavita is a cross platform reading server. Opening an ebook with malicious scripts inside leads to code execution inside the browsing context. Kavita doesn't sanitize or sandbox the contents of epubs, allowing scripts inside ebooks to execute. This vulnerability was patched in version 0.8.1.	2024-06-28	3.5	CVE-2024-39307
LabVantage--LIMS	A vulnerability was found in LabVantage LIMS 2017. It has been declared as problematic. This vulnerability affects unknown code of the file /labvantage/rc?command=file&file=WEB-CORE/elements/files/filesembedded.jsp of the component POST Request Handler. The manipulation of the argument sdcid/keyid1/keyid2/keyid3 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-269800. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-27	3.5	CVE-2024-6367
LabVantage--LIMS	A vulnerability was found in LabVantage LIMS 2017. It has been rated as problematic. This issue affects some unknown processing of the file /labvantage/rc?command=page of the component POST Request Handler. The manipulation of the argument param1 leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-269801 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-27	3.5	CVE-2024-6368
LabVantage--LIMS	A vulnerability classified as problematic has been found in LabVantage LIMS 2017. Affected is an unknown function of the file /labvantage/rc?command=page&sdcid=LV_ReagentLot of the component POST Request Handler. The manipulation of the argument mode 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-269802 is the identifier assigned to this vulnerability.	2024-06-27	3.5	CVE-2024-6369
LabVantage--LIMS	A vulnerability classified as problematic was found in LabVantage LIMS 2017. Affected by this vulnerability is an unknown functionality of the file /labvantage/rc?command=file&file=WEB-OPAL/pagetypes/bulletins/sendbulletin.jsp of the component POST Request Handler. The manipulation of the argument bulletinbody leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to	2024-06-27	3.5	CVE-2024-6370

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the public and may be used. The associated identifier of this vulnerability is VDB-269803.			
lahirudanushka--School Management System	A vulnerability was found in lahirudanushka School Management System 1.0.0/1.0.1 and classified as problematic. This issue affects some unknown processing of the file /subject.php of the component Subject Page. The manipulation of the argument Subject Title/Sybillus Details 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-269807.	2024-06-27	3.5	CVE-2024-6374
NixOS--nix	Nix is a package manager for Linux and other Unix systems that makes package management reliable and reproducible. A build process has access to and can change the permissions of the build directory. After creating a setuid binary in a globally accessible location, a malicious local user can assume the permissions of a Nix daemon worker and hijack all future builds. This issue was patched in version(s) 2.23.1, 2.22.2, 2.21.3, 2.20.7, 2.19.5 and 2.18.4.	2024-06-28	3.6	CVE-2024-38531
octobercms--october	October is a self-hosted CMS platform based on the Laravel PHP Framework. This issue affects authenticated administrators who may be redirected to an untrusted URL using the PageFinder schema. The resolver for the page finder link schema (`october://`) allowed external links, therefore allowing an open redirect outside the scope of the active host. This vulnerability has been patched in version 3.5.15.	2024-06-26	3.5	CVE-2024-24764
octobercms--october	October is a self-hosted CMS platform based on the Laravel PHP Framework. The X-October-Request-Handler Header does not sanitize the AJAX handler name and allows unescaped HTML to be reflected back. There is no impact since this vulnerability cannot be exploited through normal browser interactions. This unescaped value is only detectable when using a proxy interception tool. This issue has been patched in version 3.5.15.	2024-06-26	3.1	CVE-2024-25637
The Conduit Contributors--Conduit	Incomplete cleanup when performing redactions in Conduit, allowing an attacker to check whether certain strings were present in the PDU before redaction	2024-06-25	3.7	CVE-2024-6300
udn--udn News App	udn News Android APP stores the user session in logcat file when user log into the APP. A malicious APP or an attacker with physical access to the Android device can retrieve this session and use it to log into the news APP and other services provided by udn.	2024-06-25	3.9	CVE-2024-6294
udn--udn News App	udn News Android APP stores the unencrypted user session in the local database when user log into the application. A malicious APP or an attacker with physical access to the Android device can retrieve this session and use it to log into the news APP and other services provided by udn.	2024-06-25	3.9	CVE-2024-6295
ZKTeco--ZKBio CVSecurity V5000	A vulnerability, which was classified as problematic, was found in ZKTeco ZKBio CVSecurity V5000 4.1.0. This affects an unknown part of the component Push Configuration Section. The manipulation of the argument Configuration Name leads to cross site scripting. It is possible to initiate the attack remotely. The identifier VDB-269733 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-06-26	2.4	CVE-2024-6344