SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 04 September 2024

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-43955	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Themeum Droip allows File Manipulation.This issue affects Droip: from n/a through 1.1.1.	10.0	More Details
CVE-2024-43918	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WBW WBW Product Table PRO allows SQL Injection.This issue affects WBW Product Table PRO: from n/a through 1.9.4.	10.0	More Details
CVE-2024-8030	The Ultimate Store Kit Elementor Addons, Woocommerce Builder, EDD Builder, Elementor Store Builder, Product Grid, Product Table, Woocommerce Slider plugin is vulnerable to PHP Object Injection via deserialization of untrusted input via the _ultimate_store_kit_wishlist cookie in versions up to , and including, 2.0.3. This makes it possible for an unauthenticated attacker to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker or above to delete arbitrary files, retrieve sensitive data, or execute code.	9.8	More Details
CVE-2024-45508	HTMLDOC before 1.9.19 has an out-of-bounds write in parse_paragraph in ps-pdf.cxx because of an attempt to strip leading whitespace from a whitespace-only node.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41364	RPi-Jukebox-RFID v2.7.0 was discovered to contain a remote code execution (RCE) vulnerability via htdocs\trackEdit.php	9.8	More Details
CVE-2024-41366	RPi-Jukebox-RFID v2.7.0 was discovered to contain a remote code execution (RCE) vulnerability via htdocs\userScripts.php	9.8	More Details
CVE-2024-41367	RPi-Jukebox-RFID v2.7.0 was discovered to contain a remote code execution (RCE) vulnerability via htdocs\api\playlist\appendFileToPlaylist.php	9.8	More Details
CVE-2024-41368	RPi-Jukebox-RFID v2.7.0 was discovered to contain a remote code execution (RCE) vulnerability via htdocs\inc.setWlanIpMail.php	9.8	More Details
CVE-2024-41369	RPi-Jukebox-RFID v2.7.0 was discovered to contain a remote code execution (RCE) vulnerability via htdocs\inc.setWifi.php	9.8	More Details
CVE-2024-41370	Organizr v1.90 was discovered to contain a SQL injection vulnerability via chat/setlike.php.	9.8	More Details
CVE-2024-41372	Organizr v1.90 was discovered to contain a SQL injection vulnerability via chat/settyping.php.	9.8	More Details
CVE-2024-6670	In WhatsUp Gold versions released before 2024.0.0, a SQL Injection vulnerability allows an unauthenticated attacker to retrieve the users encrypted password.	9.8	More Details
CVE-2024-6671	In WhatsUp Gold versions released before 2024.0.0, if the application is configured with only a single user, a SQL Injection vulnerability allows an unauthenticated attacker to retrieve the users encrypted password.	9.8	More Details
CVE-2024-45488	One Identity Safeguard for Privileged Passwords before 7.5.2 allows unauthorized access because of an issue related to cookies. This only affects virtual appliance installations (VMware or HyperV). The fixed versions are 7.0.5.1 LTS, 7.4.2, and 7.5.2.	9.8	More Details
CVE-2024-45491	An issue was discovered in libexpat before 2.6.3. dtdCopy in xmlparse.c can have an integer overflow for nDefaultAtts on 32-bit platforms (where UINT_MAX equals SIZE_MAX).	9.8	More Details
CVE-2024-45492	An issue was discovered in libexpat before 2.6.3. nextScaffoldPart in xmlparse.c can have an integer overflow for m_groupSize on 32-bit platforms (where UINT_MAX equals SIZE_MAX).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45522	Linen before cd37c3e does not verify that the domain is linen.dev or www.linen.dev when resetting a password. This occurs in create in apps/web/pages/api/forgot-password/index.ts.	9.8	More Details
CVE-2024-34198	TOTOLINK AC1200 Wireless Router A3002RU V2.1.1-B20230720.1011 is vulnerable to Buffer Overflow. The formWlEncrypt CGI handler in the boa program fails to limit the length of the wlan_ssid field from user input. This allows attackers to craft malicious HTTP requests by supplying an excessively long value for the wlan_ssid field, leading to a stack overflow. This can be further exploited to execute arbitrary commands or launch denial-of-service attacks.	9.8	More Details
CVE-2024-43772	SQL Injection in download student learning course function of Easytest Online Test Platform ver.24E01 and earlier allow remote attackers to execute arbitrary SQL commands via the uid parameter.	9.8	More Details
CVE-2024-43773	SQL Injection in download class learning course function of Easytest Online Test Platform ver.24E01 and earlier allow remote attackers to execute arbitrary SQL commands via the cstr parameter.	9.8	More Details
CVE-2024-6919	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in NAC Telecommunication Systems Inc. NACPremium allows Blind SQL Injection.This issue affects NACPremium: through 01082024.	9.8	More Details
CVE-2024-45622	ASIS (aka Aplikasi Sistem Sekolah using CodeIgniter 3) 3.0.0 through 3.2.0 allows index.php username SQL injection for Authentication Bypass.	9.8	More Details
CVE-2024-45623	D-Link DAP-2310 Hardware A Firmware 1.16RC028 allows remote attackers to execute arbitrary code via a stack-based buffer overflow in the ATP binary that handles PHP HTTP GET requests for the Apache HTTP Server (httpd). NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	9.8	More Details
CVE-2024-7261	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device.	9.8	More Details
CVE-2024-44921	SeaCMS v12.9 was discovered to contain a SQL injection vulnerability via the id parameter at /dmplayer/dmku/index.php?ac=del.	9.8	More Details
CVE-2024-8381	A potentially exploitable type confusion could be triggered when looking up a property name on an object being used as the `with` environment. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, Firefox ESR < 115.15, Thunderbird < 128.2, and Thunderbird < 115.15.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8384	The JavaScript garbage collector could mis-color cross-compartment objects if OOM conditions were detected at the right point between two passes. This could have led to memory corruption. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, Firefox ESR < 115.15, Thunderbird < 128.2, and Thunderbird < 115.15.	9.8	More Details
CVE-2024-8385	A difference in the handling of StructFields and ArrayTypes in WASM could be used to trigger an exploitable type confusion vulnerability. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, and Thunderbird < 128.2.	9.8	More Details
CVE-2024-8387	Memory safety bugs present in Firefox 129, Firefox ESR 128.1, and Thunderbird 128.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, and Thunderbird < 128.2.	9.8	More Details
CVE-2024-8389	Memory safety bugs present in Firefox 129. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 130.	9.8	More Details
CVE-2024-4259	Improper Privilege Management vulnerability in SAMPAŞ Holding AKOS allows Collect Data as Provided by Users.This issue affects AKOS: through 20240902. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2024-41433	PingCAP TiDB v8.1.0 was discovered to contain a buffer overflow via the component expression.ExplainExpressionList. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input. NOTE: PingCAP maintains that the actual reproduction of this issue did not cause the security impact of service interruption to other users. They argue that this is a complex query bug and not a DoS vulnerability.	9.8	More Details
CVE-2024-41361	RPi-Jukebox-RFID v2.7.0 was discovered to contain a remote code execution (RCE) vulnerability via htdocs\manageFilesFolders.php	9.8	More Details
CVE-2024-44809	A remote code execution (RCE) vulnerability exists in the Pi Camera project, version 1.0, maintained by RECANTHA. The issue arises from improper sanitization of user input passed to the "position" GET parameter in the tilt.php script. An attacker can exploit this by sending crafted input data that includes malicious command sequences, allowing arbitrary commands to be executed on the server with the privileges of the web server user. This vulnerability is exploitable remotely and poses significant risk if the application is exposed to untrusted networks.	9.8	More Details
CVE-2024-29731	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/app/ax/checkBlindFields/ , parameters idChallenge and idEmpresa.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29729	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/app/ax/generateShortURL/, parameter url.	9.8	More Details
CVE-2024-29728	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/app/ax/inscribeUsuario/ , parameter idDesafio.	9.8	More Details
CVE-2024-4428	Improper Privilege Management vulnerability in Menulux Information Technologies Managment Portal allows Collect Data as Provided by Users.This issue affects Managment Portal: through 21.05.2024.	9.8	More Details
CVE-2024-29727	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/app/ax/sendParticipationRemember/ , parameter send.	9.8	More Details
CVE-2024-29726	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/app/ax/setAsRead/, parameter id.	9.8	More Details
CVE-2024-29725	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/app/ax/sort_bloques/, parameter list.	9.8	More Details
CVE-2024-29724	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/ax/registerSp/, parameter idDesafio.	9.8	More Details
CVE-2024-29723	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/conexiones/ax/openTracExt/, parameter categoria;.	9.8	More Details
CVE-2024-7857	The Media Library Folders plugin for WordPress is vulnerable to second order SQL Injection via the 'sort_type' parameter of the 'mlf_change_sort_type' AJAX action in all versions up to, and including, 8.2.2 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 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.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45435	Chartist 1.x through 1.3.0 allows Prototype Pollution via the extend function.	9.8	More Details
CVE-2024-45233	An issue was discovered in powermail extension through 12.3.5 for TYPO3. Several actions in the OutputController can directly be called, due to missing or insufficiently implemented access checks, resulting in Broken Access Control. Depending on the configuration of the Powermail Frontend plugins, an unauthenticated attacker can exploit this to edit, update, delete, or export data of persisted forms. This can only be exploited when the Powermail Frontend plugins are used. The fixed versions are 7.5.0, 8.5.0, 10.9.0, and 12.4.0.	9.8	More Details
CVE-2024-34195	TOTOLINK AC1200 Wireless Router A3002R Firmware V1.1.1-B20200824 is vulnerable to Buffer Overflow. In the boa server program's CGI handling function formWlEncrypt, there is a lack of length restriction on the wlan_ssid field. This oversight leads to potential buffer overflow under specific circumstances. For instance, by invoking the formWlanRedirect function with specific parameters to alter wlan_idx's value and subsequently invoking the formWlEncrypt function, an attacker can trigger buffer overflow, enabling arbitrary command execution or denial of service attacks.	9.8	More Details
CVE-2024-44761	An issue in EQ Enterprise Management System before v2.0.0 allows attackers to execute a directory traversal via crafted requests.	9.8	More Details
CVE-2024-43931	Deserialization of Untrusted Data vulnerability in eyecix JobSearch allows Object Injection.This issue affects JobSearch: from n/a through 2.5.3.	9.8	More Details
CVE-2024-42905	Beijing Digital China Cloud Technology Co., Ltd. DCME-320 v.7.4.12.60 has a command execution vulnerability, which can be exploited to obtain device administrator privileges via the getVar function in the code/function/system/tool/ping.php file.	9.8	More Details
CVE-2024-8255	Delta Electronics DTN Soft version 2.0.1 and prior are vulnerable to an attacker achieving remote code execution through a deserialization of untrusted data vulnerability.	9.8	More Details
CVE-2024-29730	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/app/ax/consejoRandom/ , parameter idCat;.	9.8	More Details
CVE-2024-44778	A reflected cross-site scripting (XSS) vulnerability in the parent parameter in the index page of vTiger CRM 7.4.0 allows attackers to execute arbitrary code in the context of a user's browser via injecting a crafted payload.	9.6	More Details
CVE-2024-44777	A reflected cross-site scripting (XSS) vulnerability in the tag parameter in the index page of vTiger CRM 7.4.0 allows attackers to execute arbitrary code in the context of a user's browser via injecting a crafted payload.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44779	A reflected cross-site scripting (XSS) vulnerability in the viewname parameter in the index page of vTiger CRM 7.4.0 allows attackers to execute arbitrary code in the context of a user's browser via injecting a crafted payload.	9.6	More Details
CVE-2024-5057	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Easy Digital Downloads allows SQL Injection.This issue affects Easy Digital Downloads: from n/a through 3.2.12.	9.3	More Details
CVE-2024-38795	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CridioStudio ListingPro allows SQL Injection.This issue affects ListingPro: from n/a through 2.9.4.	9.3	More Details
CVE-2024-39622	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CridioStudio ListingPro.This issue affects ListingPro: from n/a through 2.9.4.	9.3	More Details
CVE-2024-39653	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in E4J s.R.L. VikRentCar allows SQL Injection.This issue affects VikRentCar: from n/a through 1.4.0.	9.3	More Details
CVE-2024-43132	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPWeb Elite Docket (WooCommerce Collections / Wishlist / Watchlist) allows SQL Injection.This issue affects Docket (WooCommerce Collections / Wishlist / Watchlist): from n/a before 1.7.0.	9.3	More Details
CVE-2024-43144	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in StylemixThemes Cost Calculator Builder allows SQL Injection.This issue affects Cost Calculator Builder: from n/a through 3.2.15.	9.3	More Details
CVE-2024-43917	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in TemplateInvaders TI WooCommerce Wishlist allows SQL Injection.This issue affects TI WooCommerce Wishlist: from n/a through 2.8.2.	9.3	More Details
CVE-2024-43941	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Propovoice Propovoice Pro allows SQL Injection.This issue affects Propovoice Pro: from n/a through 1.7.0.3.	9.3	More Details
CVE-2024-8016	The Events Calendar Pro plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 7.0.2 via deserialization of untrusted input from the 'filters' parameter in widgets. This makes it possible for authenticated attackers, with administrator-level access and above, to inject a PHP Object. The additional presence of a POP chain allows attackers to execute code remotely. In certain configurations, this can be exploitable by lower level users. We confirmed that this plugin installed with Elementor makes it possible for users with contributor-level access and above to exploit this issue.	9.1	More Details
CVE-2024-3673	The Web Directory Free WordPress plugin before 1.7.3 does not validate a parameter before using it in an include(), which could lead to Local File Inclusion issues.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7856	The MP3 Audio Player – Music Player, Podcast Player & Radio by Sonaar plugin for WordPress is vulnerable to unauthorized arbitrary file deletion due to a missing capability check on the removeTempFiles() function and insufficient path validation on the 'file' parameter in all versions up to, and including, 5.7.0.1. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary files which can make remote code execution possible when wp-config.php is deleted.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-28100	eLabFTW is an open source electronic lab notebook for research labs. By uploading specially crafted files, a regular user can create a circumstance where a visitor's browser runs arbitrary JavaScript code in the context of the eLabFTW application. This can be triggered by the visitor viewing a list of experiments. Viewing this allows the malicious script to act on behalf of the visitor in any way, including the creation of API keys for persistence, or other options normally available to the user. If the user viewing the page has the sysadmin role in eLabFTW, the script can act as a sysadmin (including system configuration and extensive user management roles). Users are advised to upgrade to at least version 5.0.0. There are no known workarounds for this vulnerability.	8.9	More Details
CVE-2024-8226	A vulnerability has been found in Tenda O1 1.0.0.7(10648) and classified as critical. Affected by this vulnerability is the function formSetCfm of the file /goform/setcfm. The manipulation of the argument funcpara1 leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-8329	6SHR system from Gether Technology does not properly validate the specific page parameter, allowing remote attackers with regular privilege to inject SQL command to read, modify, and delete database contents.	8.8	More Details
CVE-2024-7435	The Attire theme for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 2.0.6 via deserialization of untrusted input. 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.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8227	A vulnerability was found in Tenda O1 1.0.0.7(10648) and classified as critical. Affected by this issue is the function fromDhcpSetSer of the file /goform/DhcpSetSer. The manipulation of the argument dhcpStartIp/dhcpEndIp/dhcpGw/dhcpMask/dhcpLeaseTime/dhcpDns1/dhcpDns2 leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-8252	The Clean Login plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.14.5 via the 'template' attribute of the clean-login-register shortcode. 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.	8.8	More Details
CVE-2024-2694	The Betheme theme for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 27.5.6 via deserialization of untrusted input of the 'mfn-page-items' post meta value. 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 plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	8.8	More Details
CVE-2024-8330	6SHR system from Gether Technology does not properly validate uploaded file types, allowing remote attackers with regular privileges to upload web shell scripts and use them to execute arbitrary system commands on the server.	8.8	More Details
CVE-2024-8327	Easy test Online Learning and Testing Platform from HWA JIUH DIGITAL TECHNOLOGY does not properly validate a specific page parameter, allowing remote attackers with regular privilege to inject arbitrary SQL commands to read, modify, and delete database contents.	8.8	More Details
CVE-2024-41157	in OpenHarmony v4.1.0 and prior versions allow a local attacker cause the common permission is upgraded to root and sensitive information leak through use after free.	8.8	More Details
CVE-2024-6672	In WhatsUp Gold versions released before 2024.0.0, a SQL Injection vulnerability allows an authenticated low-privileged attacker to achieve privilege escalation by modifying a privileged user's password.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43804	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. An OS Command Injection vulnerability allows any authenticated user on the application to execute arbitrary code on the web application server via port scanning functionality. User-supplied input is used without validation when constructing and executing an OS command. User supplied JSON POST data is parsed and if "id" JSON key does not exist, JSON value supplied via "ip" JSON key is assigned to the "ip" variable. Later on, "ip" variable which can be controlled by the attacker is used when constructing the cmd and cmd1 strings without any extra validation. Then, server_mod.subprocess_execute function is called on both cmd1 and cmd2. When the definition of the server_mod.subprocess_execute() function is analyzed, it can be seen that subprocess.Popen() is called on the input parameter with shell=True which results in OS Command Injection. This issue has not yet been patched. Users are advised to contact the Roxy-WI to coordinate a fix.	8.8	More Details
CVE-2024-7607	The Front End Users plugin for WordPress is vulnerable to time-based SQL Injection via the ‘order’ parameter in all versions up to, and including, 3.2.28 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.	8.8	More Details
CVE-2024-8198	Heap buffer overflow in Skia in Google Chrome prior to 128.0.6613.113 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-8194	Type Confusion in V8 in Google Chrome prior to 128.0.6613.113 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-8193	Heap buffer overflow in Skia in Google Chrome prior to 128.0.6613.113 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-7717	The WP Events Manager plugin for WordPress is vulnerable to time-based SQL Injection via the ‘order’ parameter in all versions up to, and including, 2.1.11 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.	8.8	More Details
CVE-2024-41160	in OpenHarmony v4.1.0 and prior versions allow a local attacker cause the common permission is upgraded to root and sensitive information leak through use after free.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45048	PHPSpreadsheet is a pure PHP library for reading and writing spreadsheet files. Affected versions are subject to a bypassing of a filter which allows for an XXE-attack. This in turn allows attacker to obtain contents of local files, even if error reporting is muted. This vulnerability has been addressed in release version 2.2.1. All users are advised to upgrade. There are no known workarounds for this vulnerability.	8.8	More Details
CVE-2024-43774	SQL Injection in download personal learning course function of Easytest Online Test Platform ver.24E01 and earlier allow remote authenticated users to execute arbitrary SQL commands via the uid parameter.	8.8	More Details
CVE-2024-43775	SQL Injection in search course titles function of Easytest Online Test Platform ver.24E01 and earlier allow remote authenticated users to execute arbitrary SQL commands via the search parameter.	8.8	More Details
CVE-2024-43776	SQL Injection in mock exam function of Easytest Online Test Platform ver.24E01 and earlier allow remote authenticated users to execute arbitrary SQL commands via the qlevel parameter.	8.8	More Details
CVE-2024-7871	SQL Injection in online dictionary function of Easytest Online Test Platform ver.24E01 and earlier allow remote authenticated users to execute arbitrary SQL commands via the word parameter.	8.8	More Details
CVE-2024-38811	VMware Fusion (13.x before 13.6) contains a code-execution vulnerability due to the usage of an insecure environment variable. A malicious actor with standard user privileges may exploit this vulnerability to execute code in the context of the Fusion application.	8.8	More Details
CVE-2024-45586	This vulnerability exists due to improper access controls on APIs in the Authentication module of Symphony XTS Web Trading and Mobile Trading platforms (version 2.0.0.1_P160). An authenticated remote attacker could exploit this vulnerability by manipulating parameters through HTTP request which could lead to unauthorized account take over belonging to other users.	8.8	More Details
CVE-2024-45587	This vulnerability exists in Symphony XTS Web Trading platform version 2.0.0.1_P160 due to improper access controls on APIs in the Transaction module of vulnerable application. An authenticated remote attacker could exploit this vulnerability by manipulating parameters through HTTP request which could lead to compromise of other user accounts.	8.8	More Details
CVE-2024-8382	Internal browser event interfaces were exposed to web content when privileged EventHandler listener callbacks ran for those events. Web content that tried to use those interfaces would not be able to use them with elevated privileges, but their presence would indicate certain browser features had been used, such as when a user opened the Dev Tools console. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, Firefox ESR < 115.15, Thunderbird < 128.2, and Thunderbird < 115.15.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49233	Insufficient access checks in Visual Planning Admin Center 8 before v.1 Build 240207 allow attackers in possession of a non-administrative Visual Planning account to utilize functions normally reserved for administrators. The affected functions allow attackers to obtain different types of configured credentials and potentially elevate their privileges to administrator level.	8.8	More Details
CVE-2024-42902	An issue in the js_localize.php function of LimeSurvey v6.6.2 and before allows attackers to execute arbitrary code via injecting a crafted payload into the lng parameter of the js_localize.php function	8.8	More Details
CVE-2024-45307	SudoBot, a Discord moderation bot, is vulnerable to privilege escalation and exploit of the `-config` command in versions prior to 9.26.7. Anyone is theoretically able to update any configuration of the bot and potentially gain control over the bot's settings. Every version of v9 before v9.26.7 is affected. Other versions (e.g. v8) are not affected. Users should upgrade to version 9.26.7 to receive a patch. A workaround would be to create a command permission overwrite in the Database. A SQL statement provided in the GitHub Security Advisor can be executed to create a overwrite that disallows users without `ManageGuild` permission to run the `-config` command. Run the SQL statement for every server the bot is in, and replace `<guild_id>` with the appropriate Guild ID each time.	8.8	More Details
CVE-2024-45394	Authenticator is a browser extension that generates two-step verification codes. In versions 7.0.0 and below, encryption keys for user data were stored encrypted at-rest using only AES-256 and the EVP_BytesToKey KDF. Therefore, attackers with a copy of a user's data are able to brute-force the user's encryption key. Users on version 8.0.0 and above are automatically migrated away from the weak encoding on first login. Users should destroy encrypted backups made with versions prior to 8.0.0.	8.8	More Details
CVE-2024-7970	Out of bounds write in V8 in Google Chrome prior to 128.0.6613.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-45059	i-Educar is free, fully online school management software that can be used by school secretaries, teachers, coordinators, and area managers. A SQL Injection vulnerability was found prior to the 2.9 branch in the `ieducar/intranet/funcionario_vinculo_det.php` file, which creates the query by concatenating the unsanitized GET parameter `cod_func`, allowing the attacker to obtain sensitive information such as emails and password hashes. Commit 7824b95745fa2da6476b9901041d9c854bf52ffe fixes the issue.	8.8	More Details
CVE-2024-8362	Use after free in WebAudio in Google Chrome prior to 128.0.6613.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-45346	A code execution vulnerability exists in the XiaomiGetApps application product. This vulnerability is caused by the verification logic being bypassed, and an attacker can exploit this vulnerability to execute malicious code.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8228	A vulnerability was found in Tenda O5 1.0.0.8(5017). It has been classified as critical. This affects the function fromSafeSetMacFilter of the file /goform/setMacFilterList. The manipulation of the argument remark/type/time leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-8229	A vulnerability was found in Tenda O6 1.0.0.7(2054). It has been declared as critical. This vulnerability affects the function frommacFilterModify of the file /goform/operateMacFilter. The manipulation of the argument mac leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2023-26324	A code execution vulnerability exists in the XiaomiGetApps application product. This vulnerability is caused by the verification logic being bypassed, and an attacker can exploit this vulnerability to execute malicious code.	8.8	More Details
CVE-2023-26322	A code execution vulnerability exists in the XiaomiGetApps application product. This vulnerability is caused by the verification logic being bypassed, and an attacker can exploit this vulnerability to execute malicious code.	8.8	More Details
CVE-2024-8231	A vulnerability classified as critical has been found in Tenda O6 1.0.0.7(2054). Affected is the function fromVirtualSet of the file /goform/setPortForward. The manipulation of the argument ip/localPort/publicPort/app 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. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-8230	A vulnerability was found in Tenda O6 1.0.0.7(2054). It has been rated as critical. This issue affects the function fromSafeSetMacFilter of the file /goform/setMacFilterList. The manipulation of the argument remark/type/time leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-8004	A stored Cross-site Scripting (XSS) vulnerability affecting ENOVIA Collaborative Industry Innovator from Release 3DEXPERIENCE R2022x through Release 3DEXPERIENCE R2024x allows an attacker to execute arbitrary script code in user's browser session.	8.7	More Details
CVE-2024-7932	A stored Cross-site Scripting (XSS) vulnerability affecting 3DDashboard in 3DSwymer on Release 3DEXPERIENCE R2024x allows an attacker to execute arbitrary script code in user's browser session.	8.7	More Details
CVE-2024-7938	A stored Cross-site Scripting (XSS) vulnerability affecting 3DDashboard in 3DSwymer from Release 3DEXPERIENCE R2023x through Release 3DEXPERIENCE R2024x allows an attacker to execute arbitrary script code in user's browser session.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7939	A stored Cross-site Scripting (XSS) vulnerability affecting 3DSwym in 3DSwymer on Release 3DEXPERIENCE R2024x allows an attacker to execute arbitrary script code in user's browser session.	8.7	More Details
CVE-2024-20446	A vulnerability in the DHCPv6 relay agent of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling of specific fields in a DHCPv6 RELAY-REPLY message. An attacker could exploit this vulnerability by sending a crafted DHCPv6 packet to any IPv6 address that is configured on an affected device. A successful exploit could allow the attacker to cause the dhcp_snoop process to crash and restart multiple times, causing the affected device to reload and resulting in a DoS condition.	8.6	More Details
CVE-2024-38793	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in PriceListo Best Restaurant Menu by PriceListo allows SQL Injection.This issue affects Best Restaurant Menu by PriceListo: from n/a through 1.4.1.	8.5	More Details
CVE-2024-39638	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Roundup WP Registrations for the Events Calendar allows SQL Injection.This issue affects Registrations for the Events Calendar: from n/a through 2.12.2.	8.5	More Details
CVE-2024-39620	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CridioStudio ListingPro allows SQL Injection.This issue affects ListingPro: from n/a through 2.9.4.	8.5	More Details
CVE-2024-43943	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Wpsoul Greenshift Woocommerce Addon allows SQL Injection.This issue affects Greenshift Woocommerce Addon: from n/a before 1.9.8.	8.5	More Details
CVE-2024-43942	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Wpsoul Greenshift Query and Meta Addon allows SQL Injection.This issue affects Greenshift Query and Meta Addon: from n/a before 3.9.2.	8.5	More Details
CVE-2024-23365	Memory corruption while releasing shared resources in MinkSocket listener thread.	8.4	More Details
CVE-2024-33047	Memory corruption when the captureRead QDCM command is invoked from user-space.	8.4	More Details
CVE-2024-33060	Memory corruption when two threads try to map and unmap a single node simultaneously.	8.4	More Details
CVE-2024-33035	Memory corruption while calculating total metadata size when a very high reserved size is requested by gralloc clients.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39816	in OpenHarmony v4.1.0 and prior versions allow a local attacker arbitrary code execution in pre-installed apps through out-of-bounds write.	8.4	More Details
CVE-2024-33045	Memory corruption when BTFM client sends new messages over Slimbus to ADSP.	8.4	More Details
CVE-2024-38386	in OpenHarmony v4.1.0 and prior versions allow a local attacker arbitrary code execution in pre-installed apps through out-of-bounds write.	8.4	More Details
CVE-2024-6204	Zohocorp ManageEngine Exchange Reporter Plus versions before 5715 are vulnerable to SQL Injection in the reports module.	8.3	More Details
CVE-2024-5546	Zohocorp ManageEngine Password Manager Pro versions before 12431 and ManageEngine PAM360 versions before 7001 are affected by authenticated SQL Injection vulnerability via a global search option.	8.3	More Details
CVE-2021-38121	Insufficient or weak TLS protocol version identified in Advance authentication client server communication when specific service is accessed between devices. This issue affects NetIQ Advance Authentication versions before 6.3.5.1	8.3	More Details
CVE-2024-7654	An ActiveMQ Discovery service was reachable by default from an OpenEdge Management installation when an OEE/OEM auto-discovery feature was activated. Unauthorized access to the discovery service's UDP port allowed content injection into parts of the OEM web interface making it possible for other types of attack that could spoof or deceive web interface users. Unauthorized use of the OEE/OEM discovery service was remediated by deactivating the discovery service by default.	8.3	More Details
CVE-2024-7345	Local ABL Client bypass of the required PASOE security checks may allow an attacker to commit unauthorized code injection into Multi-Session Agents on supported OpenEdge LTS platforms up to OpenEdge LTS 11.7.18 and LTS 12.2.13 on all supported release platforms	8.3	More Details
CVE-2021-22530	A vulnerability identified in NetIQ Advance Authentication that doesn't enforce account lockout when brute force attack is performed on API based login. This issue may lead to user account compromise if successful or may impact server performance. This issue impacts all NetIQ Advance Authentication before 6.3.5.1	8.2	More Details
CVE-2024-23359	Information disclosure while decoding Tracking Area Update Accept or Attach Accept message received from network.	8.2	More Details
CVE-2024-43965	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Smackcoders SendGrid for WordPress allows SQL Injection.This issue affects SendGrid for WordPress: from n/a through 1.4.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39584	Dell Client Platform BIOS contains a Use of Default Cryptographic Key Vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Secure Boot bypass and arbitrary code execution.	8.2	More Details
CVE-2024-42057	A command injection vulnerability in the IPSec VPN feature of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an unauthenticated attacker to execute some OS commands on an affected device by sending a crafted username to the vulnerable device. Note that this attack could be successful only if the device was configured in User-Based-PSK authentication mode and a valid user with a long username exceeding 28 characters exists.	8.1	More Details
CVE-2021-22509	A vulnerability identified in storing and reusing information in Advance Authentication. This issue can lead to leakage of sensitive data to unauthorized user. The issue affects NetIQ Advance Authentication before 6.3.5.1	8.1	More Details
CVE-2024-45588	This vulnerability exists in Symphony XTS Web Trading platform version 2.0.0.1_P160 due to improper access controls on APIs in the Preference module of the application. An authenticated remote attacker could exploit this vulnerability by manipulating parameters through HTTP request which could lead to unauthorized access and modification of sensitive information belonging to other users.	8.1	More Details
CVE-2024-41964	Kirby is a CMS targeting designers and editors. Kirby allows to restrict the permissions of specific user roles. Users of that role can only perform permitted actions. Permissions for creating and deleting languages have already existed and could be configured, but were not enforced by Kirby's frontend or backend code. A permission for updating existing languages has not existed before the patched versions. So disabling the languages.* wildcard permission for a role could not have prohibited updates to existing language definitions. The missing permission checks allowed attackers with Panel access to manipulate the language definitions. The problem has been patched in Kirby 3.6.6.6, Kirby 3.7.5.5, Kirby 3.8.4.4, Kirby 3.9.8.2, Kirby 3.10.1.1, and Kirby 4.3.1. Please update to one of these or a later version to fix the vulnerability. There are no known workarounds for this vulnerability.	8.1	More Details
CVE-2024-39747	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 uses default credentials for potentially critical functionality.	8.1	More Details
CVE-2024-42991	MCMS v5.4.1 has front-end file upload vulnerability which can lead to remote command execution.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45058	i-Educar is free, fully online school management software that can be used by school secretaries, teachers, coordinators, and area managers. Prior to the 2.9 branch, an attacker with only minimal viewing privileges in the settings section is able to change their user type to Administrator (or another type with super-permissions) through a specifically crafted POST request to `/intranet/educar_usuario_cad.php`, modifying the `nivel_usuario_` parameter. The vulnerability occurs in the file located at `ieducar/intranet/educar_usuario_cad.php`, which does not check the user's current permission level before allowing changes. Commit c25910cdf11ab50e50162a49dd44bef544422b6e contains a patch for the issue.	8.1	More Details
CVE-2024-42793	A Cross-Site Request Forgery (CSRF) vulnerability was found in Kashipara Music Management System v1.0 via a crafted request to the /music/ajax.php?action=save_user page.	8.0	More Details
CVE-2024-5622	An untrusted search path vulnerability in the AprolConfigureCCServices of B&R APROL <= R 4.2.-07P3 and <= R 4.4-00P3 may allow an authenticated local attacker to execute arbitrary code with elevated privileges.	7.8	More Details
CVE-2024-38456	HIGH-LEIT V05.08.01.03 and HIGH-LEIT V04.25.00.00 to 4.25.01.01 for Windows from Vivavis contain an insecure file and folder permissions vulnerability in prunsrv.exe. A regular user (non-admin) can exploit the weak folder and file permissions to escalate privileges and execute arbitrary code in the context of NT AUTHORITY\SYSTEM.	7.8	More Details
CVE-2024-38401	Memory corruption while processing concurrent IOCTL calls.	7.8	More Details
CVE-2024-38402	Memory corruption while processing IOCTL call for getting group info.	7.8	More Details
CVE-2024-44945	In the Linux kernel, the following vulnerability has been resolved: netfilter: nfnetlink: Initialise extack before use in ACKs Add missing extack initialisation when ACKing BATCH_BEGIN and BATCH_END.	7.8	More Details
CVE-2024-8374	UltiMaker Cura slicer versions 5.7.0-beta.1 through 5.7.2 are vulnerable to code injection via the 3MF format reader (/plugins/ThreeMFReader.py). The vulnerability arises from improper handling of the drop_to_buildplate property within 3MF files, which are ZIP archives containing the model data. When a 3MF file is loaded in Cura, the value of the drop_to_buildplate property is passed to the Python eval() function without proper sanitization, allowing an attacker to execute arbitrary code by crafting a malicious 3MF file. This vulnerability poses a significant risk as 3MF files are commonly shared via 3D model databases.	7.8	More Details
CVE-2024-33052	Memory corruption when user provides data for FM HCI command control operations.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33038	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA.	7.8	More Details
CVE-2024-6473	Yandex Browser for Desktop before 24.7.1.380 has a DLL Hijacking Vulnerability because an untrusted search path is used.	7.8	More Details
CVE-2024-43700	xfpt versions prior to 1.01 fails to handle appropriately some parameters inside the input data, resulting in a stack-based buffer overflow vulnerability. When a user of the affected product is tricked to process a specially crafted file, arbitrary code may be executed on the user's environment.	7.8	More Details
CVE-2024-3655	Use After Free vulnerability in Arm Ltd Bifrost GPU Kernel Driver, Arm Ltd Valhall GPU Kernel Driver, Arm Ltd Arm 5th Gen GPU Architecture Kernel Driver allows a local non-privileged user to make improper GPU memory processing operations to gain access to already freed memory.This issue affects Bifrost GPU Kernel Driver: from r43p0 through r49p0; Valhall GPU Kernel Driver: from r43p0 through r49p0; Arm 5th Gen GPU Architecture Kernel Driver: from r43p0 through r49p0.	7.8	More Details
CVE-2024-8250	NTLMSSP dissector crash in Wireshark 4.2.0 to 4.0.6 and 4.0.0 to 4.0.16 allows denial of service via packet injection or crafted capture file	7.8	More Details
CVE-2024-33042	Memory corruption when Alternative Frequency offset value is set to 255.	7.8	More Details
CVE-2024-33054	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine.	7.8	More Details
CVE-2024-5623	An untrusted search path vulnerability in B&R APROL <= R 4.4-00P3 may be used by an authenticated local attacker to get other users to execute arbitrary code under their privileges.	7.8	More Details
CVE-2024-4555	Improper Privilege Management vulnerability in OpenText NetIQ Access Manager allows user account impersonation in specific scenario. This issue affects NetIQ Access Manager before 5.0.4.1 and before 5.1	7.7	More Details
CVE-2024-38693	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in weDevs WP User Frontend allows SQL Injection.This issue affects WP User Frontend: from n/a through 4.0.7.	7.6	More Details
CVE-2024-39658	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Salon Booking System Salon booking system allows SQL Injection.This issue affects Salon booking system: from n/a through 10.7.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43805	jupyterlab is an extensible environment for interactive and reproducible computing, based on the Jupyter Notebook Architecture. This vulnerability depends on user interaction by opening a malicious notebook with Markdown cells, or Markdown file using JupyterLab preview feature. A malicious user can access any data that the attacked user has access to as well as perform arbitrary requests acting as the attacked user. JupyterLab v3.6.8, v4.2.5 and Jupyter Notebook v7.2.2 have been patched to resolve this issue. Users are advised to upgrade. There is no workaround for the underlying DOM Clobbering susceptibility. However, select plugins can be disabled on deployments which cannot update in a timely fashion to minimise the risk. These are: 1. `@jupyterlab/mathjax-extension:plugin` - users will loose ability to preview mathematical equations. 2. `@jupyterlab/markdownviewer-extension:plugin` - users will loose ability to open Markdown previews. 3. `@jupyterlab/mathjax2-extension:plugin` (if installed with optional `jupyterlab-mathjax2` package) - an older version of the mathjax plugin for JupyterLab 4.x. To disable these extensions run: ```jupyter labextension disable @jupyterlab/markdownviewer-extension:plugin && jupyter labextension disable @jupyterlab/mathjax-extension:plugin && jupyter labextension disable @jupyterlab/mathjax2-extension:plugin ``` in bash.	7.6	More Details
CVE-2024-38868	Zohocorp ManageEngine Endpoint Central affected by Incorrect authorization vulnerability while isolating the devices.This issue affects Endpoint Central: before 11.3.2406.08 and before 11.3.2400.15	7.6	More Details
CVE-2023-26323	A code execution vulnerability exists in the Xiaomi App market product. The vulnerability is caused by unsafe configuration and can be exploited by attackers to execute arbitrary code.	7.6	More Details
CVE-2024-33051	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length.	7.5	More Details
CVE-2024-41435	YugabyteDB v2.21.1.0 was discovered to contain a buffer overflow via the "insert into" parameter.	7.5	More Details
CVE-2024-41436	ClickHouse v24.3.3.102 was discovered to contain a buffer overflow via the component DB::evaluateConstantExpressionImpl.	7.5	More Details
CVE-2024-33050	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	7.5	More Details
CVE-2024-5148	A flaw was found in the gnome-remote-desktop package. The gnome-remote-desktop system daemon performs inadequate validation of session agents using D-Bus methods related to transitioning a client connection from the login screen to the user session. As a result, the system RDP TLS certificate and key can be exposed to unauthorized users. This flaw allows a malicious user on the system to take control of the RDP client connection during the login screen-to-user session transition.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45391	Tina is an open-source content management system (CMS). Sites building with Tina CMS's command line interface (CLI) prior to version 1.6.2 that use a search token may be vulnerable to the search token being leaked via lock file (tina-lock.json). Administrators of Tina-enabled websites with search setup should rotate their key immediately. This issue has been patched in @tinacms/cli version 1.6.2. Upgrading and rotating the search token is required for the proper fix.	7.5	More Details
CVE-2024-23358	Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in Modem.	7.5	More Details
CVE-2024-45436	extractFromZipFile in model.go in Ollama before 0.1.47 can extract members of a ZIP archive outside of the parent directory.	7.5	More Details
CVE-2024-6119	Issue summary: Applications performing certificate name checks (e.g., TLS clients checking server certificates) may attempt to read an invalid memory address resulting in abnormal termination of the application process. Impact summary: Abnormal termination of an application can a cause a denial of service. Applications performing certificate name checks (e.g., TLS clients checking server certificates) may attempt to read an invalid memory address when comparing the expected name with an `otherName` subject alternative name of an X.509 certificate. This may result in an exception that terminates the application program. Note that basic certificate chain validation (signatures, dates, ...) is not affected, the denial of service can occur only when the application also specifies an expected DNS name, Email address or IP address. TLS servers rarely solicit client certificates, and even when they do, they generally don't perform a name check against a reference identifier (expected identity), but rather extract the presented identity after checking the certificate chain. So TLS servers are generally not affected and the severity of the issue is Moderate. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue.	7.5	More Details
CVE-2024-1621	The registration process of uniFLOW Online (NT-ware product) apps, prior to and including version 2024.1.0, can be compromised when email login is enabled on the tenant. Those tenants utilising email login in combination with Microsoft Safe Links or similar are impacted. This vulnerability may allow the attacker to register themselves against a genuine user in the system and allow malicious users with similar access and capabilities via the app to the existing genuine user.	7.5	More Details
CVE-2024-8234	** UNSUPPORTED WHEN ASSIGNED ** A command injection vulnerability in the functions formSysCmd(), formUpgradeCert(), and formDelcert() in the Zyxel NWA1100-N firmware version 1.00(AACE.1)C0 could allow an unauthenticated attacker to execute some OS commands to access system files on an affected device.	7.5	More Details
CVE-2024-6232	There is a MEDIUM severity vulnerability affecting CPython. Regular expressions that allowed excessive backtracking during tarfile.TarFile header parsing are vulnerable to ReDoS via specifically-crafted tar archives.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5412	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device.	7.5	More Details
CVE-2024-23364	Transient DOS when processing the non-transmitted BSSID profile sub-elements present within the MBSSID Information Element (IE) of a beacon frame that is received from over-the-air (OTA).	7.5	More Details
CVE-2024-42058	A null pointer dereference vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V5.20 through V5.38, and USG20(W)-VPN series firmware versions from V5.20 through V5.38 could allow an unauthenticated attacker to cause DoS conditions by sending crafted packets to a vulnerable device.	7.5	More Details
CVE-2024-8383	Firefox normally asks for confirmation before asking the operating system to find an application to handle a scheme that the browser does not support. It did not ask before doing so for the Usenet-related schemes news: and snews:. Since most operating systems don't have a trusted newsreader installed by default, an unscrupulous program that the user downloaded could register itself as a handler. The website that served the application download could then launch that application at will. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, and Firefox ESR < 115.15.	7.5	More Details
CVE-2024-20089	In wlan, there is a possible denial of service due to incorrect error handling. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08861558; Issue ID: MSV-1526.	7.5	More Details
CVE-2024-6921	Cleartext Storage of Sensitive Information vulnerability in NAC Telecommunication Systems Inc. NACPremium allows Retrieve Embedded Sensitive Data.This issue affects NACPremium: through 01082024.	7.5	More Details
CVE-2024-33048	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	7.5	More Details
CVE-2024-45388	Hoverfly is a lightweight service virtualization/ API simulation / API mocking tool for developers and testers. The `/api/v2/simulation` POST handler allows users to create new simulation views from the contents of a user-specified file. This feature can be abused by an attacker to read arbitrary files from the Hoverfly server. Note that, although the code prevents absolute paths from being specified, an attacker can escape out of the `hf.Cfg.ResponsesBodyFilesPath` base path by using `../` segments and reach any arbitrary files. This issue was found using the Uncontrolled data used in path expression CodeQL query for python. Users are advised to make sure the final path (`filepath.Join(hf.Cfg.ResponsesBodyFilesPath, filePath)`) is contained within the expected base path (`filepath.Join(hf.Cfg.ResponsesBodyFilesPath, "/")`). This issue is also tracked as GHSL-2023-274.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45311	Quinn is a pure-Rust, async-compatible implementation of the IETF QUIC transport protocol. As of quinn-proto 0.11, it is possible for a server to `accept()`, `retry()`, `refuse()`, or `ignore()` an `Incoming` connection. However, calling `retry()` on an unvalidated connection exposes the server to a likely panic in the following situations: 1. Calling `refuse` or `ignore` on the resulting validated connection, if a duplicate initial packet is received. This issue can go undetected until a server's `refuse()`/`ignore()` code path is exercised, such as to stop a denial of service attack. 2. Accepting when the initial packet for the resulting validated connection fails to decrypt or exhausts connection IDs, if a similar initial packet that successfully decrypts and doesn't exhaust connection IDs is received. This issue can go undetected if clients are well-behaved. The former situation was observed in a real application, while the latter is only theoretical.	7.5	More Details
CVE-2024-33057	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location.	7.5	More Details
CVE-2024-44760	Incorrect access control in the component /servlet/SnoopServlet of Shenzhou News Union Enterprise Management System v5.0 through v18.8 allows attackers to access sensitive information regarding the server.	7.5	More Details
CVE-2024-45490	An issue was discovered in libexpat before 2.6.3. xmlparse.c does not reject a negative length for XML_ParseBuffer.	7.5	More Details
CVE-2024-34017	Local privilege escalation due to DLL hijacking vulnerability. The following products are affected: Acronis Snap Deploy (Windows) before build 4569.	7.3	More Details
CVE-2024-34019	Local privilege escalation due to DLL hijacking vulnerability. The following products are affected: Acronis Snap Deploy (Windows) before build 4569.	7.3	More Details
CVE-2024-8343	A vulnerability, which was classified as critical, was found in SourceCodester Sentiment Based Movie Rating System 1.0. Affected is an unknown function of the file /classes/Users.php?f=save_client of the component User Registration Handler. The manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-8301	A vulnerability was found in dingfanzu CMS up to 29d67d9044f6f93378e6eb6ff92272217ff7225c. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /ajax/checkin.php. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42471	actions/artifact is the GitHub ToolKit for developing GitHub Actions. Versions of `actions/artifact` before 2.1.7 are vulnerable to arbitrary file write when using `downloadArtifactInternal`, `downloadArtifactPublic`, or `streamExtractExternal` for extracting a specifically crafted artifact that contains path traversal filenames. Users are advised to upgrade to version 2.1.7 or higher. There are no known workarounds for this issue.	7.3	More Details
CVE-2024-45390	@blakeembrey/template is a string template library. Prior to version 1.2.0, it is possible to inject and run code within the template if the attacker has access to write the template name. Version 1.2.0 contains a patch. As a workaround, don't pass untrusted input as the template display name, or don't use the display name feature.	7.3	More Details
CVE-2024-8340	A vulnerability classified as critical has been found in SourceCodester Electric Billing Management System 1.0. This affects an unknown part of the file /Actions.php?a=login. 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.	7.3	More Details
CVE-2024-6586	Lightdash version 0.1024.6 allows users with the necessary permissions, such as Administrator or Editor, to create and share dashboards. A dashboard that contains HTML elements which point to a threat actor controlled source can trigger an SSRF request when exported, via a POST request to /api/v1/dashboards//export. The forged request contains the value of the exporting user's session token. A threat actor could obtain the session token of any user who exports the dashboard. The obtained session token can be used to perform actions as the victim on the application, resulting in session takeover.	7.3	More Details
CVE-2024-4554	Improper Input Validation vulnerability in OpenText NetIQ Access Manager leads to Cross-Site Scripting (XSS) attack. This issue affects NetIQ Access Manager before 5.0.4.1 and 5.1.	7.3	More Details
CVE-2024-8368	A vulnerability was found in code-projects Hospital 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.	7.3	More Details
CVE-2024-42060	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted internal user agreement file to the vulnerable device.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2440	The Theme Editor plugin for WordPress is vulnerable to deserialization of untrusted input via the 'images_array' parameter in versions up to, and including 2.8. This makes it possible for authenticated attackers with administrative privileges to call files using a PHAR wrapper that will deserialize and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.	7.2	More Details
CVE-2024-44916	Vulnerability in admin_ip.php in Seacms v13.1, when action=set, allows attackers to control IP parameters that are written to the data/admin/ip.php file and could result in arbitrary command execution.	7.2	More Details
CVE-2024-6311	The Funnelforms Free plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'af2_add_font' function in all versions up to, and including, 3.7.3.2. This makes it possible for authenticated attackers, with administrator-level and above permissions, to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.2	More Details
CVE-2024-41236	A SQL injection vulnerability in /smsa/admin_login.php in Kashipara Responsive School Management System v3.2.0 allows an attacker to execute arbitrary SQL commands via the "username" parameter of the Admin Login Page	7.2	More Details
CVE-2024-7346	Host name validation for TLS certificates is bypassed when the installed OpenEdge default certificates are used to perform the TLS handshake for a networked connection. This has been corrected so that default certificates are no longer capable of overriding host name validation and will need to be replaced where full TLS certificate validation is needed for network security. The existing certificates should be replaced with CA-signed certificates from a recognized certificate authority that contain the necessary information to support host name validation.	7.2	More Details
CVE-2024-42059	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V5.00 through V5.38, USG FLEX series firmware versions from V5.00 through V5.38, USG FLEX 50(W) series firmware versions from V5.00 through V5.38, and USG20(W)-VPN series firmware versions from V5.00 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted compressed language file via FTP.	7.2	More Details
CVE-2024-7203	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.60 through V5.38 and USG FLEX series firmware versions from V4.60 through V5.38 could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands on an affected device by executing a crafted CLI command.	7.2	More Details
CVE-2023-45896	ntfs3 in the Linux kernel through 6.8.0 allows a physically proximate attacker to read kernel memory by mounting a filesystem (e.g., if a Linux distribution is configured to allow unprivileged mounts of removable media) and then leveraging local access to trigger an out-of-bounds read. A length value can be larger than the amount of memory allocated. NOTE: the supplier's perspective is that there is no vulnerability when an attack requires an attacker-modified filesystem image.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43958	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Gianni Porto IntoTheDark allows Reflected XSS.This issue affects IntoTheDark: from n/a through 1.0.5.	7.1	More Details
CVE-2024-43948	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Dinesh Karki WP Armour Extended.This issue affects WP Armour Extended: from n/a through 1.26.	7.1	More Details
CVE-2024-43963	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WaspThemes YellowPencil Visual CSS Style Editor allows Reflected XSS.This issue affects YellowPencil Visual CSS Style Editor: from n/a through 7.6.1.	7.1	More Details
CVE-2024-23362	Cryptographic issue while parsing RSA keys in COBR format.	7.1	More Details
CVE-2024-43950	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Nextbricks Brickscore allows Stored XSS.This issue affects Brickscore: from n/a through 1.4.2.5.	7.1	More Details
CVE-2024-43926	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Beaver Builder Team Beaver Builder allows Reflected XSS.This issue affects Beaver Builder: from n/a through 2.8.3.2.	7.1	More Details
CVE-2024-5784	The Tutor LMS Pro plugin for WordPress is vulnerable to unauthorized administrative actions execution due to a missing capability checks on multiple functions like treport_quiz_atttempt_delete and tutor_gc_class_action in all versions up to, and including, 2.7.2. This makes it possible for authenticated attackers, with the subscriber-level access and above, to preform an administrative actions on the site, like comments, posts or users deletion, viewing notifications, etc.	7.1	More Details
CVE-2024-43921	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Magic Post Thumbnail allows Reflected XSS.This issue affects Magic Post Thumbnail: from n/a through 5.2.9.	7.1	More Details
CVE-2024-33016	memory corruption when an invalid firehose patch command is invoked.	6.8	More Details
CVE-2024-35133	IBM Security Verify Access 10.0.0 through 10.0.8 OIDC Provider could allow a remote authenticated attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim.	6.8	More Details
CVE-2024-39771	QBiC CLOUD CC-2L v1.1.30 and earlier and Safie One v1.8.2 and earlier do not properly validate certificates, which may allow a network-adjacent unauthenticated attacker to obtain and/or alter communications of the affected product via a man-in-the-middle attack.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37136	Dell Path to PowerProtect, versions 1.1, 1.2, contains an Exposure of Private Personal Information to an Unauthorized Actor vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to information exposure.	6.8	More Details
CVE-2024-20411	A vulnerability in Cisco NX-OS Software could allow an authenticated, local attacker with privileges to access the Bash shell to execute arbitrary code as root on an affected device. This vulnerability is due to insufficient security restrictions when executing commands from the Bash shell. An attacker with privileges to access the Bash shell could exploit this vulnerability by executing a specific crafted command on the underlying operating system. A successful exploit could allow the attacker to execute arbitrary code with the privileges of root.	6.7	More Details
CVE-2024-2881	Fault Injection vulnerability in wc_ed25519_sign_msg function in wolfssl/wolfcrypt/src/ed25519.c in WolfSSL wolfssl5.6.6 on Linux/Windows allows remote attacker co-resides in the same system with a victim process to disclose information and escalate privileges via Rowhammer fault injection to the ed25519_key structure.	6.7	More Details
CVE-2024-20086	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1551.	6.7	More Details
CVE-2024-20087	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1550.	6.7	More Details
CVE-2023-43078	Dell Dock Firmware and Dell Client Platform contain an Improper Link Resolution vulnerability during installation resulting in arbitrary folder deletion, which could lead to Privilege Escalation or Denial of Service.	6.7	More Details
CVE-2024-39579	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contains an incorrect privilege assignment vulnerability. A local high privileged attacker could potentially exploit this vulnerability to gain root-level access.	6.7	More Details
CVE-2024-20413	A vulnerability in Cisco NX-OS Software could allow an authenticated, local attacker with privileges to access the Bash shell to elevate privileges to network-admin on an affected device. This vulnerability is due to insufficient security restrictions when executing application arguments from the Bash shell. An attacker with privileges to access the Bash shell could exploit this vulnerability by executing crafted commands on the underlying operating system. A successful exploit could allow the attacker to create new users with the privileges of network-admin.	6.7	More Details
CVE-2024-39775	in OpenHarmony v4.1.0 and prior versions allow a remote attacker cause information leak through out-of-bounds Read.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45308	HedgeDoc is an open source, real-time, collaborative, markdown notes application. When using HedgeDoc 1 with MySQL or MariaDB, it is possible to create notes with an alias matching the ID of existing notes. The affected existing note can then not be accessed anymore and is effectively hidden by the new one. When the freeURL feature is enabled (by setting the `allowFreeURL` config option or the `CMD_ALLOW_FREEURL` environment variable to `true`), any user with the appropriate permissions can create a note with an arbitrary alias, e.g. by accessing it in the browser. When MySQL or MariaDB are used, it is possible to create a new note with an alias that matches the lower-cased ID of a different note. HedgeDoc then always presents the new note to users, as these databases perform case-insensitive matching and the lower-cased alias is found first. This issue only affects HedgeDoc instances that use MySQL or MariaDB. Depending on the permission settings of the HedgeDoc instance, the issue can be exploited only by logged-in users or by all (including non-logged-in) users. The exploit requires knowledge of the ID of the target note. Attackers could use this issue to present a manipulated copy of the original note to the user, e.g. by replacing the links with malicious ones. Attackers can also use this issue to prevent access to the original note, causing a denial of service. No data is lost, as the original content of the affected notes is still present in the database. Users are advised to upgrade to version 1.10.0 which addresses this issue. Users unable to upgrade may disable freeURL mode which prevents the exploitation of this issue. The impact can also be limited by restricting freeURL note creation to trusted, logged-in users by enabling `requireFreeURLAuthentication`/`CMD_REQUIRE_FREEURL_AUTHENTICATION`.	6.5	More Details
CVE-2024-6312	The Funnelforms Free plugin for WordPress is vulnerable to arbitrary file deletion in all versions up to, and including, 3.7.3.2 via the 'af2DeleteFontFile' function. This is due to the plugin not properly validating a file or its path prior to deleting it. This makes it possible for unauthenticated attackers to delete arbitrary files, including the wp-config.php file, which can make site takeover and remote code execution possible.	6.5	More Details
CVE-2024-7744	In WS_FTP Server versions before 8.8.8 (2022.0.8), an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in the Web Transfer Module allows File Discovery, Probe System Files, User-Controlled Filename, Path Traversal. An authenticated file download flaw has been identified where a user can craft an API call that allows them to download a file from an arbitrary folder on the drive where that user host's root folder is located (by default this is C:)	6.5	More Details
CVE-2024-44930	Serilog before v2.1.0 was discovered to contain a Client IP Spoofing vulnerability, which allows attackers to falsify their IP addresses by specifying an arbitrary IP as a value of X-Forwarded-For or Client-Ip headers while performing HTTP requests.	6.5	More Details
CVE-2024-7745	In WS_FTP Server versions before 8.8.8 (2022.0.8), a Missing Critical Step in Multi-Factor Authentication of the Web Transfer Module allows users to skip the second-factor verification and log in with username and password only.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42903	A Host header injection vulnerability in the password reset function of LimeSurvey v.6.6.1+240806 and before allows attackers to send users a crafted password reset link that will direct victims to a malicious domain.	6.5	More Details
CVE-2024-6449	HyperView Geoportal Toolkit in versions lower than 8.5.0 does not restrict cross-domain requests when fetching remote content pointed by one of GET request parameters. An unauthenticated remote attacker can prepare links, which upon opening will load scripts from a remote location controlled by the attacker and execute them in the user space. By manipulating this parameter it is also possible to enumerate some of the devices in Local Area Network in which the server resides.	6.5	More Details
CVE-2024-45509	In MISP through 2.4.196, app/Controller/BookmarksController.php does not properly restrict access to bookmarks data in the case where the user is not an org admin.	6.5	More Details
CVE-2024-20478	A vulnerability in the software upgrade component of Cisco Application Policy Infrastructure Controller (APIC) and Cisco Cloud Network Controller, formerly Cisco Cloud APIC, could allow an authenticated, remote attacker with Administrator-level privileges to install a modified software image, leading to arbitrary code injection on an affected system. This vulnerability is due to insufficient signature validation of software images. An attacker could exploit this vulnerability by installing a modified software image. A successful exploit could allow the attacker to execute arbitrary code on the affected system and elevate their privileges to root. Note: Administrators should always validate the hash of any upgrade image before uploading it to Cisco APIC and Cisco Cloud Network Controller.	6.5	More Details
CVE-2024-43964	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Michael Leithold DSGVO All in one for WP allows Stored XSS.This issue affects DSGVO All in one for WP: from n/a through 4.5.	6.5	More Details
CVE-2024-43961	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in azurecurve azurecurve Toggle Show/Hide allows Stored XSS.This issue affects azurecurve Toggle Show/Hide: from n/a through 2.1.3.	6.5	More Details
CVE-2024-43936	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPDeveloper EmbedPress allows Stored XSS.This issue affects EmbedPress: from n/a through 4.0.8.	6.5	More Details
CVE-2024-43953	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Classic Addons Classic Addons – WPBakery Page Builder allows Stored XSS.This issue affects Classic Addons – WPBakery Page Builder: from n/a through 3.0.	6.5	More Details
CVE-2024-43952	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Esotera allows Stored XSS.This issue affects Esotera: from n/a through 1.2.5.1.	6.5	More Details
CVE-2024-43951	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Tempera allows Stored XSS.This issue affects Tempera: from n/a through 1.8.2.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43949	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Automattic GHActivity allows Stored XSS.This issue affects GHActivity: from n/a through 2.0.0-alpha.	6.5	More Details
CVE-2024-43946	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in SKT Themes SKT Blocks – Gutenberg based Page Builder allows Stored XSS.This issue affects SKT Blocks – Gutenberg based Page Builder: from n/a through 1.5.	6.5	More Details
CVE-2024-43935	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Delicious Delicious Recipes – WordPress Recipe Plugin allows Stored XSS.This issue affects Delicious Recipes – WordPress Recipe Plugin: from n/a through 1.6.7.	6.5	More Details
CVE-2024-43934	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Robert Felty Collapsing Archives allows Stored XSS.This issue affects Collapsing Archives: from n/a through 3.0.5.	6.5	More Details
CVE-2024-4629	A vulnerability was found in Keycloak. This flaw allows attackers to bypass brute force protection by exploiting the timing of login attempts. By initiating multiple login requests simultaneously, attackers can exceed the configured limits for failed attempts before the system locks them out. This timing loophole enables attackers to make more guesses at passwords than intended, potentially compromising account security on affected systems.	6.5	More Details
CVE-2024-43957	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Sk. Abul Hasan Animated Number Counters allows PHP Local File Inclusion.This issue affects Animated Number Counters: from n/a through 1.9.	6.5	More Details
CVE-2024-43940	Missing Authorization vulnerability in VIICTORY MEDIA LLC Z Y N I T H allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Z Y N I T H: from n/a through 7.4.9.	6.5	More Details
CVE-2024-43939	Missing Authorization vulnerability in VIICTORY MEDIA LLC Z Y N I T H allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Z Y N I T H: from n/a through 7.4.9.	6.5	More Details
CVE-2024-43920	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jegstudio Gutenverse allows Stored XSS.This issue affects Gutenverse: from n/a through 1.9.4.	6.5	More Details
CVE-2024-8108	The Share This Image plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'alignment' parameter in all versions up to, and including, 2.01 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.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8276	The WPZOOM Portfolio Lite – Filterable Portfolio Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘align’ attribute within the 'wp:wpzoom-blocks' Gutenberg block in all versions up to, and including, 1.4.4 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.	6.4	More Details
CVE-2024-45389	Pagefind, a fully static search library, initializes its dynamic JavaScript and WebAssembly files relative to the location of the first script the user loads. This information is gathered by looking up the value of `document.currentScript.src`. Prior to Pagefind version 1.1.1, it is possible to "clobber" this lookup with otherwise benign HTML on the page. This will cause `document.currentScript.src` to resolve as an external domain, which will then be used by Pagefind to load dependencies. This exploit would only work in the case that an attacker could inject HTML to a live, hosted, website. In these cases, this would act as a way to escalate the privilege available to an attacker. This assumes they have the ability to add some elements to the page (for example, `img` tags with a `name` attribute), but not others, as adding a `script` to the page would itself be the cross-site scripting vector. Pagefind has tightened this resolution in version 1.1.1 by ensuring the source is loaded from a valid script element. There are no reports of this being exploited in the wild via Pagefind.	6.4	More Details
CVE-2024-7895	The Beaver Builder – WordPress Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘type’ parameter in all versions up to, and including, 2.8.3.5 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.	6.4	More Details
CVE-2024-7122	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple widgets in all versions up to, and including, 1.13.6 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.	6.4	More Details
CVE-2024-7606	The Front End Users plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'user-search' shortcode in all versions up to, and including, 3.2.28 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.	6.4	More Details
CVE-2024-5879	The HubSpot – CRM, Email Marketing, Live Chat, Forms & Analytics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' attribute of the HubSpot Meeting Widget in all versions up to, and including, 11.1.22 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.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3998	The Betheme theme for WordPress is vulnerable to Stored Cross-Site Scripting via several of the plugin's shortcodes in all versions up to, and including, 27.5.6 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.	6.4	More Details
CVE-2024-1384	The Premium Portfolio Features for Phlox theme plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'aux_recent_portfolios_grid' shortcode in all versions up to, and including, 2.3.3 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.	6.4	More Details
CVE-2024-5061	The Enfold - Responsive Multi-Purpose Theme theme for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘wrapper_class’ and 'class' parameters in all versions up to, and including, 6.0.3 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.	6.4	More Details
CVE-2024-4401	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘id’ and 'eae_slider_animation' parameters in all 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 access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1056	The FunnelKit Funnel Builder Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'allow_iframe_tag_in_post' function which uses the 'wp_kses_allowed_html' filter to globally allow script and iframe tags in posts in all versions up to, and including, 3.4.5. 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.	6.4	More Details
CVE-2024-43792	Halo is an open source website building tool. A security vulnerability has been identified in versions prior to 2.17.0 of the Halo project. This vulnerability allows an attacker to execute malicious scripts in the user's browser through specific HTML and JavaScript code, potentially leading to a Cross-Site Scripting (XSS) attack. Users are advised to upgrade to version 2.17.0+. There are no known workarounds for this vulnerability.	6.3	More Details
CVE-2024-8342	A vulnerability, which was classified as critical, has been found in SourceCodester Petshop Management System 1.0. This issue affects some unknown processing of the file /controllers/add_client.php. The manipulation of the argument image_profile leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8344	A vulnerability has been found in Campcodes Supplier Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/edit_area.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.	6.3	More Details
CVE-2021-22529	A vulnerability identified in NetIQ Advance Authentication that leaks sensitive server information. This issue affects NetIQ Advance Authentication version before 6.3.5.1	6.3	More Details
CVE-2024-43797	audiobookshelf is a self-hosted audiobook and podcast server. A non-admin user is not allowed to create libraries (or access only the ones they have permission to). However, the `LibraryController` is missing the check for admin user and thus allows a path traversal issue. Allowing non-admin users to write to any directory in the system can be seen as a form of path traversal. However, since it can be restricted to only admin permissions, fixing this is relatively simple and falls more into the realm of Role-Based Access Control (RBAC). This issue has been addressed in release version 2.13.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	6.3	More Details
CVE-2024-8346	A vulnerability classified as critical has been found in SourceCodester Computer Laboratory Management System 1.0. Affected is the function update_settings_info of the file /classes/SystemSettings.php?f=update_settings. The manipulation of the argument name leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-8347	A vulnerability classified as critical was found in SourceCodester Computer Laboratory Management System 1.0. Affected by this vulnerability is the function delete_record of the file /classes/Master.php?f=delete_record. 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.	6.3	More Details
CVE-2024-8348	A vulnerability, which was classified as critical, has been found in SourceCodester Computer Laboratory Management System 1.0. Affected by this issue is the function delete_category of the file /classes/Master.php?f=delete_category. 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.	6.3	More Details
CVE-2024-8380	A vulnerability was found in SourceCodester Contact Manager with Export to VCF 1.0. It has been rated as critical. This issue affects some unknown processing of the file /endpoint/delete-account.php of the component Delete Contact Handler. The manipulation of the argument contact leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-39578	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.1 contains a UNIX symbolic link (symlink) following vulnerability. A local high privileged attacker could potentially exploit this vulnerability, leading to denial of service, information tampering.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8345	A vulnerability was found in SourceCodester Music Gallery Site 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /classes/Users.php?f=delete. 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.	6.3	More Details
CVE-2024-8336	A vulnerability classified as critical was found in SourceCodester Music Gallery Site 1.0. Affected by this vulnerability is an unknown functionality of the file /php-music/classes/Master.php?f=delete_music. 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.	6.3	More Details
CVE-2024-8331	A vulnerability was found in OpenRapid RapidCMS up to 1.3.1. It has been classified as critical. This affects an unknown part of the file /admin/user/user-move-run.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.	6.3	More Details
CVE-2024-8339	A vulnerability was found in SourceCodester Electric Billing Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /?page=tracks of the component Connection Code Handler. The manipulation of the argument code leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-8303	A vulnerability classified as critical has been found in dingfanzu CMS up to 29d67d9044f6f93378e6eb6ff92272217ff7225c. This affects an unknown part of the file /ajax/getBasicInfo.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. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-8296	A vulnerability was found in FeehiCMS up to 2.1.1 and classified as critical. This issue affects the function insert of the file /admin/index.php?r=user%2Fcreate. The manipulation of the argument User[avatar] leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-8335	A vulnerability classified as critical has been found in OpenRapid RapidCMS up to 1.3.1. Affected is an unknown function of the file /resource/runlogon.php. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-8294	A vulnerability, which was classified as critical, was found in FeehiCMS up to 2.1.1. This affects the function update of the file /admin/index.php?r=friendly-link%2Fupdate. The manipulation of the argument FriendlyLink[image] leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43954	Incorrect Authorization vulnerability in Themeum Droip allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Droip: from n/a through 1.1.1.	6.3	More Details
CVE-2024-45045	Collabora Online is a collaborative online office suite based on LibreOffice technology. In the mobile (Android/iOS) device variants of Collabora Online it was possible to inject JavaScript via url encoded values in links contained in documents. Since the Android JavaScript interface allows access to internal functions, the likelihood that the app could be compromised via this vulnerability is considered high. Non-mobile variants are not affected. Mobile variants should update to the latest version provided by the platform appstore. There are no known workarounds for this vulnerability.	6.3	More Details
CVE-2024-8341	A vulnerability classified as critical was found in SourceCodester Petshop Management System 1.0. This vulnerability affects unknown code of the file /controllers/add_user.php. The manipulation of the argument avatar leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-8302	A vulnerability was found in dingfanzu CMS up to 29d67d9044f6f93378e6eb6ff92272217ff7225c. It has been rated as critical. Affected by this issue is some unknown functionality of the file /ajax/chpwd.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. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-8338	A vulnerability was found in HFO4 shudong-share 2.4.7. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /includes/fileReceive.php of the component File Extension Handler. The manipulation of the argument file leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2024-7858	The Media Library Folders plugin for WordPress is vulnerable to unauthorized access due to missing capability checks on several AJAX functions in the media-library-plus.php file in all versions up to, and including, 8.2.3. This makes it possible for authenticated attackers, with subscriber-level access and above, to perform several actions related to managing media files and folder along with controlling settings.	6.3	More Details
CVE-2024-8295	A vulnerability has been found in FeehiCMS up to 2.1.1 and classified as critical. This vulnerability affects the function createBanner of the file /admin/index.php?r=banner%2Fbanner-create. The manipulation of the argument BannerForm[img] leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8332	A vulnerability was found in master-nan Sweet-CMS up to 5f441e022b8876f07cde709c77b5be6d2f262e3f. It has been declared as critical. This vulnerability affects unknown code of the file /table/index. The manipulation leads to sql injection. The attack can be initiated remotely. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The name of the patch is 146359646a5a90cb09156dbd0013b7df77f2aa6c. It is recommended to apply a patch to fix this issue.	6.3	More Details
CVE-2023-26321	A path traversal vulnerability exists in the Xiaomi File Manager application product(international version). The vulnerability is caused by unfiltered special characters and can be exploited by attackers to overwrite and execute code in the file.	6.3	More Details
CVE-2021-38122	A Cross-Site Scripting vulnerable identified in NetIQ Advance Authentication that impacts the server functionality and disclose sensitive information. This issue affects NetIQ Advance Authentication before 6.3.5.1	6.2	More Details
CVE-2024-8365	Vault Community Edition and Vault Enterprise experienced a regression where functionality that HMAC'd sensitive headers in the configured audit device, specifically client tokens and token accessors, was removed. This resulted in the plaintext values of client tokens and token accessors being stored in the audit log. This vulnerability, CVE-2024-8365, was fixed in Vault Community Edition and Vault Enterprise 1.17.5 and Vault Enterprise 1.16.9.	6.2	More Details
CVE-2024-8235	A flaw was found in libvirt. A refactor of the code fetching the list of interfaces for multiple APIs introduced a corner case on platforms where allocating 0 bytes of memory results in a NULL pointer. This corner case would lead to a NULL-pointer dereference and subsequent crash of virtinterfaced. This issue could allow clients connecting to the read-only socket to crash the virtinterfaced daemon.	6.2	More Details
CVE-2024-5024	The Memberpress plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'mepr_screenname' and 'mepr_key' parameter in all versions up to, and including, 1.11.29 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.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45302	RestSharp is a Simple REST and HTTP API Client for .NET. The second argument to `RestRequest.AddHeader` (the header value) is vulnerable to CRLF injection. The same applies to `RestRequest.AddOrUpdateHeader` and `RestClient.AddDefaultHeader`. The way HTTP headers are added to a request is via the `HttpHeaders.TryAddWithoutValidation` method which does not check for CRLF characters in the header value. This means that any headers from a `RestSharp.RequestHeaders` object are added to the request in such a way that they are vulnerable to CRLF-injection. In general, CRLF-injection into a HTTP header (when using HTTP/1.1) means that one can inject additional HTTP headers or smuggle whole HTTP requests. If an application using the RestSharp library passes a user-controllable value through to a header, then that application becomes vulnerable to CRLF-injection. This is not necessarily a security issue for a command line application like the one above, but if such code were present in a web application then it becomes vulnerable to request splitting (as shown in the PoC) and thus Server Side Request Forgery. Strictly speaking this is a potential vulnerability in applications using RestSharp, not in RestSharp itself, but I would argue that at the very least there needs to be a warning about this behaviour in the RestSharp documentation. RestSharp has addressed this issue in version 112.0.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	6.1	More Details
CVE-2024-6920	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NAC Telecommunication Systems Inc. NACPremium allows Stored XSS.This issue affects NACPremium: through 01082024.	6.1	More Details
CVE-2024-34577	Cross-site scripting vulnerability exists in WRC-X3000GS2-B, WRC-X3000GS2-W, and WRC-X3000GS2A-B due to improper processing of input values in easysetup.cgi. If a user views a malicious web page while logged in to the product, an arbitrary script may be executed on the user's web browser.	6.1	More Details
CVE-2024-42412	Cross-site scripting vulnerability exists in ELECOM wireless access points due to improper processing of input values in menu.cgi. If a user views a malicious web page while logged in to the product, an arbitrary script may be executed on the user's web browser.	6.1	More Details
CVE-2024-42061	A reflected cross-site scripting (XSS) vulnerability in the CGI program "dynamic_script.cgi" of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. The attacker could obtain browser-based information if the malicious script is executed on the victim’s browser.	6.1	More Details
CVE-2024-45527	REDCap 14.7.0 allows HTML injection via the project title of a New Project action. This can lead to resultant logout CSRF via index.php?logout=1, and can also be used to insert a link to an external phishing website.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44716	A cross-site scripting (XSS) vulnerability in DedeBIZ v6.3.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	6.1	More Details
CVE-2024-7692	The Flaming Forms WordPress plugin through 1.0.1 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin.	6.1	More Details
CVE-2024-7354	The Ninja Forms WordPress plugin before 3.8.11 does not escape an URL before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2024-7691	The Flaming Forms WordPress plugin through 1.0.1 does not sanitise and escape some parameters, which could allow unauthenticated users to perform Cross-Site Scripting attacks against administrators.	6.1	More Details
CVE-2024-41349	unmark 1.9.2 is vulnerable to Cross Site Scripting (XSS) via application/views/marks/add_by_url.php.	6.1	More Details
CVE-2024-41371	Organizr v1.90 is vulnerable to Cross Site Scripting (XSS) via api.php.	6.1	More Details
CVE-2024-41358	phpipam 1.6 is vulnerable to Cross Site Scripting (XSS) via app\admin\import-export\import-load-data.php.	6.1	More Details
CVE-2024-41351	bjyadmin commit a560fd5 is vulnerable to Cross Site Scripting (XSS) via Public/statics/umeditor1_2_3/php/getContent.php	6.1	More Details
CVE-2024-41350	bjyadmin commit a560fd5 is vulnerable to Cross Site Scripting (XSS) via Public/statics/umeditor1_2_3/php/imageUp.php	6.1	More Details
CVE-2024-41348	openflights commit 5234b5b is vulnerable to Cross-Site Scripting (XSS) via php/alsearch.php	6.1	More Details
CVE-2024-41347	openflights commit 5234b5b is vulnerable to Cross-Site Scripting (XSS) via php/settings.php	6.1	More Details
CVE-2024-44776	An Open Redirect vulnerability in the page parameter of vTiger CRM v7.4.0 allows attackers to redirect users to a malicious site via a crafted URL.	6.1	More Details
CVE-2024-44717	A cross-site scripting (XSS) vulnerability in DedeBIZ v6.3.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38858	Improper neutralization of input in Checkmk before version 2.3.0p14 allows attackers to inject and run malicious scripts in the Robotmk logs view.	6.1	More Details
CVE-2024-41918	'Rakuten Ichiba App' for Android 12.4.0 and earlier and 'Rakuten Ichiba App' for iOS 11.7.0 and earlier are vulnerable to improper authorization in handler for custom URL scheme. An arbitrary site may be displayed on the WebView of the product via Intent from another application installed on the user's device. As a result, the user may be redirected to an unauthorized site, and the user may become a victim of a phishing attack.	6.1	More Details
CVE-2024-5624	Reflected Cross-Site Scripting (XSS) in Shift Logbook application of B&R APROL <= R 4.4-00P3 may allow a network-based attacker to execute arbitrary JavaScript code in the context of the user's browser session	6.1	More Details
CVE-2024-8386	If a site had been granted the permission to open popup windows, it could cause Select elements to appear on top of another site to perform a spoofing attack. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, and Thunderbird < 128.2.	6.1	More Details
CVE-2024-44682	ShopXO 6.2 is vulnerable to Cross Site Scripting (XSS) in the backend that allows attackers to execute code by changing POST parameters.	6.1	More Details
CVE-2024-3886	The tagDiv Composer plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘envato_code[]’ parameter in all versions up to, and including, 5.0 due to insufficient input sanitization and output escaping within the on_ajax_check_envato_code function. 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.	6.1	More Details
CVE-2024-8260	A SMB force-authentication vulnerability exists in all versions of OPA for Windows prior to v0.68.0. The vulnerability exists because of improper input validation, allowing a user to pass an arbitrary SMB share instead of a Rego file as an argument to OPA CLI or to one of the OPA Go library’s functions.	6.1	More Details
CVE-2024-6450	HyperView Geoportal Toolkit in versions lower than 8.5.0 is vulnerable to Reflected Cross-Site Scripting (XSS). An unauthenticated attacker might trick somebody into using a crafted URL, which will cause a script to be run in user's browser.	6.1	More Details
CVE-2024-45057	i-Educar is free, fully online school management software that can be used by school secretaries, teachers, coordinators, and area managers. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the dynamic generation of HTML fields prior to the 2.9 branch. The file located at `ieducar/intranet/include/clsCampos.inc.php` does not properly validate or sanitize user-controlled input, leading to the vulnerability. Any page that uses this implementation is vulnerable, such as `intranet/educar_curso_lst.php?nm_curso=<payload>`, `intranet/atendidos_lst.php?nm_pessoa=<payload>`, `intranet/educar_abandono_tipo_lst?nome=<payload>`. Commit f2d768534aabc09b2a1fc8a5cc5f9c93925cb273 contains a patch for the issue.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44684	TpMeCMS 1.3.3.2 is vulnerable to Cross Site Scripting (XSS) in /h.php/page?ref=addtabs via the "Title," "Images," and "Content" fields.	6.1	More Details
CVE-2024-5212	The tagDiv Composer plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘envato_code[]’ parameter in all versions up to, and including, 5.0 due to insufficient input sanitization and output escaping within the on_ajax_register_forum_user function. 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.	6.1	More Details
CVE-2024-44683	Seacms v13 is vulnerable to Cross Site Scripting (XSS) via admin-video.php.	6.1	More Details
CVE-2024-42900	Ruoyi v4.7.9 and before was discovered to contain a cross-site scripting (XSS) vulnerability via the sql parameter of the createTable() function at /tool/gen/create.	6.1	More Details
CVE-2024-42904	A cross-site scripting (XSS) vulnerability in SysPass 3.2.x allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the name parameter at /Controllers/ClientController.php.	6.1	More Details
CVE-2024-44920	A cross-site scripting (XSS) vulnerability in the component admin_collect_news.php of SeaCMS v12.9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the siteurl parameter.	6.1	More Details
CVE-2024-8274	The WP Booking Calendar plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via several parameters from 'timeline_obj' in all versions up to, and including, 10.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-43986	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in MagePeople Team Taxi Booking Manager for WooCommerce allows Stored XSS.This issue affects Taxi Booking Manager for WooCommerce: through 1.0.9.	5.9	More Details
CVE-2024-8285	A flaw was found in Kroxylicious. When establishing the connection with the upstream Kafka server using a TLS secured connection, Kroxylicious fails to properly verify the server's hostname, resulting in an insecure connection. For a successful attack to be performed, the attacker needs to perform a Man-in-the-Middle attack or compromise any external systems, such as DNS or network routing configuration. This issue is considered a high complexity attack, with additional high privileges required, as the attack would need access to the Kroxylicious configuration or a peer system. The result of a successful attack impacts both data integrity and confidentiality.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45056	zksolc is a Solidity compiler for ZKsync. All LLVM versions since 2015 fold `(xor (shl 1, x), -1)` to `(rotl ~1, x)` if run with optimizations enabled. Here `~1` is generated as an unsigned 64 bits number (`2^64-1`). This number is zero-extended to 256 bits on EraVM target while it should have been sign-extended. Thus instead of producing `roti 2^256 - 1, x` the compiler produces `rotl 2^64 - 1, x`. Analysis has shown that no contracts were affected by the date of publishing this advisory. This issue has been addressed in version 1.5.3. Users are advised to upgrade and redeploy all contracts. There are no known workarounds for this vulnerability.	5.9	More Details
CVE-2024-1545	Fault Injection vulnerability in RsaPrivateDecryption function in wolfssl/wolfcrypt/src/rsa.c in WolfSSL wolfssl5.6.6 on Linux/Windows allows remote attacker co-resides in the same system with a victim process to disclose information and escalate privileges via Rowhammer fault injection to the RsaKey structure.	5.9	More Details
CVE-2024-43960	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Page Builder Addons Web and WooCommerce Addons for WPBakery Builder allows Stored XSS.This issue affects Web and WooCommerce Addons for WPBakery Builder: from n/a through 1.4.6.	5.9	More Details
CVE-2024-4556	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in OpenText NetIQ Access Manager allows access the sensitive information. This issue affects NetIQ Access Manager before 5.0.4 and before 5.1.	5.7	More Details
CVE-2024-38382	in OpenHarmony v4.0.0 and prior versions allow a local attacker cause information leak through out-of-bounds Read.	5.5	More Details
CVE-2024-33043	Transient DOS while handling PS event when Program Service name length offset value is set to 255.	5.5	More Details
CVE-2022-48944	In the Linux kernel, the following vulnerability has been resolved: sched: Fix yet more sched_fork() races Where commit 4ef0c5c6b5ba ("kernel/sched: Fix sched_fork() access an invalid sched_task_group") fixed a fork race vs cgroup, it opened up a race vs syscalls by not placing the task on the runqueue before it gets exposed through the pidhash. Commit 13765de8148f ("sched/fair: Fix fault in reweight_entity") is trying to fix a single instance of this, instead fix the whole class of issues, effectively reverting this commit.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4442	In the Linux kernel, the following vulnerability has been resolved: tcp: add sanity tests to TCP_QUEUE_SEQ Qingyu Li reported a syzkaller bug where the repro changes RCV SEQ _after_ restoring data in the receive queue. mprotect(0x4aa000, 12288, PROT_READ) = 0 mmap(0x1ffff000, 4096, PROT_NONE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x1ffff000 mmap(0x20000000, 16777216, PROT_READ|PROT_WRITE|PROT_EXEC, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x20000000 mmap(0x21000000, 4096, PROT_NONE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x21000000 socket(AF_INET6, SOCK_STREAM, IPPROTO_IP) = 3 setsockopt(3, SOL_TCP, TCP_REPAIR, [1], 4) = 0 connect(3, {sa_family=AF_INET6, sin6_port=htons(0), sin6_flowinfo=htonl(0), inet_pton(AF_INET6, "::1", &sin6_addr), sin6_scope_id=0}, 28) = 0 setsockopt(3, SOL_TCP, TCP_REPAIR_QUEUE, [1], 4) = 0 sendmsg(3, {msg_name=NULL, msg_namelen=0, msg_iov= [{iov_base="0x0000000000000003\0\0", iov_len=20}], msg_iovlen=1, msg_controllen=0, msg_flags=0}, 0) = 20 setsockopt(3, SOL_TCP, TCP_REPAIR, [0], 4) = 0 setsockopt(3, SOL_TCP, TCP_QUEUE_SEQ, [128], 4) = 0 recvfrom(3, NULL, 20, 0, NULL, NULL) = -1 ECONNRESET (Connection reset by peer) syslog shows: [111.205099] TCP recvmsg seq # bug 2: copied 80, seq 0, rcvnxt 80, fl 0 [111.207894] WARNING: CPU: 1 PID: 356 at net/ipv4/tcp.c:2343 tcp_recvmsg_locked+0x90e/0x29a0 This should not be allowed. TCP_QUEUE_SEQ should only be used when queues are empty. This patch fixes this case, and the tx path as well.	5.5	More Details
CVE-2024-44915	An issue in the component EXR!ReadEXR+0x4eef0 of Irfanview v4.67.1.0 allows attackers to cause an access violation via a crafted EXR file. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2024-44947	In the Linux kernel, the following vulnerability has been resolved: fuse: Initialize beyond-EOF page contents before setting uptodate fuse_notify_store(), unlike fuse_do_readpage(), does not enable page zeroing (because it can be used to change partial page contents). So fuse_notify_store() must be more careful to fully initialize page contents (including parts of the page that are beyond end-of-file) before marking the page uptodate. The current code can leave beyond-EOF page contents uninitialized, which makes these uninitialized page contents visible to userspace via mmap(). This is an information leak, but only affects systems which do not enable init-on-alloc (via CONFIG_INIT_ON_ALLOC_DEFAULT_ON=y or the corresponding kernel command line parameter).	5.5	More Details
CVE-2024-44914	An issue in the component EXR!ReadEXR+0x3df50 of Irfanview v4.67.1.0 allows attackers to cause an access violation via a crafted EXR file. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2024-44913	An issue in the component EXR!ReadEXR+0x40ef1 of Irfanview v4.67.1.0 allows attackers to cause an access violation via a crafted EXR file. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44944	In the Linux kernel, the following vulnerability has been resolved: netfilter: ctnetlink: use helper function to calculate expect ID Delete expectation path is missing a call to the nf_expect_get_id() helper function to calculate the expectation ID, otherwise LSB of the expectation object address is leaked to userspace.	5.5	More Details
CVE-2024-34018	Sensitive information disclosure due to insecure folder permissions. The following products are affected: Acronis Snap Deploy (Windows) before build 4569.	5.5	More Details
CVE-2024-44946	In the Linux kernel, the following vulnerability has been resolved: kcm: Serialise kcm_sendmsg() for the same socket. syzkaller reported UAF in kcm_release(). [0] The scenario is 1. Thread A builds a skb with MSG_MORE and sets kcm->seq_skb. 2. Thread A resumes building skb from kcm->seq_skb but is blocked by sk_stream_wait_memory() 3. Thread B calls sendmsg() concurrently, finishes building kcm->seq_skb and puts the skb to the write queue 4. Thread A faces an error and finally frees skb that is already in the write queue 5. kcm_release() does double-free the skb in the write queue When a thread is building a MSG_MORE skb, another thread must not touch it. Let's add a per-sk mutex and serialise kcm_sendmsg(). [0]: BUG: KASAN: slab-use-after-free in __skb_unlink include/linux/skbuff.h:2366 [inline] BUG: KASAN: slab-use-after-free in __skb_dequeue include/linux/skbuff.h:2385 [inline] BUG: KASAN: slab-use-after-free in __skb_queue_purge_reason include/linux/skbuff.h:3175 [inline] BUG: KASAN: slab-use-after-free in __skb_queue_purge include/linux/skbuff.h:3181 [inline] BUG: KASAN: slab-use-after-free in kcm_release+0x170/0x4c8 net/kcm/kcmsock.c:1691 Read of size 8 at addr ffff0000ced0fc80 by task syz-executor329/6167 CPU: 1 PID: 6167 Comm: syz-executor329 Tainted: G B 6.8.0-rc5-syzkaller-g9abbc24128bc #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/25/2024 Call trace: dump_backtrace+0x1b8/0x1e4 arch/arm64/kernel/stacktrace.c:291 show_stack+0x2c/0x3c arch/arm64/kernel/stacktrace.c:298 __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xd0/0x124 lib/dump_stack.c:106 print_address_description mm/kasan/report.c:377 [inline] print_report+0x178/0x518 mm/kasan/report.c:488 kasan_report+0xd8/0x138 mm/kasan/report.c:601 __asan_report_load8_noabort+0x20/0x2c mm/kasan/report_generic.c:381 __skb_unlink include/linux/skbuff.h:2366 [inline] __skb_dequeue include/linux/skbuff.h:2385 [inline] __skb_queue_purge_reason include/linux/skbuff.h:3175 [inline] __skb_queue_purge include/linux/skbuff.h:3181 [inline] kcm_release+0x170/0x4c8 net/kcm/kcmsock.c:1691 __sock_release net/socket.c:659 [inline] sock_close+0xa4/0x1e8 net/socket.c:1421 __fput+0x30c/0x738 fs/file_table.c:376 ____fput+0x20/0x30 fs/file_table.c:404 task_work_run+0x230/0x2e0 kernel/task_work.c:180 exit_task_work include/linux/task_work.h:38 [inline] do_exit+0x618/0x1f64 kernel/exit.c:871 do_group_exit+0x194/0x22c kernel/exit.c:1020 get_signal+0x1500/0x15ec kernel/signal.c:2893 do_signal+0x23c/0x3b44 arch/arm64/kernel/signal.c:1249 do_notify_resume+0x74/0x1f4 arch/arm64/kernel/entry-common.c:148 exit_to_user_mode_prepare arch/arm64/kernel/entry-common.c:169 [inline] exit_to_user_mode arch/arm64/kernel/entry-common.c:178 [inline] el0_svc+0xac/0x168 arch/arm64/kernel/entry-common.c:713 el0t_64_sync_handler+0x84/0xfc arch/arm64/kernel/entry-common.c:730	5.5	More Details

CVE Number	Description	Base Score	Reference
	el0t_64_sync+0x190/0x194 arch/arm64/kernel/entry.S:598 Allocated by task 6166: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x40/0x78 mm/kasan/common.c:68 kasan_save_alloc_info+0x70/0x84 mm/kasan/generic.c:626 unpoison_slab_object mm/kasan/common.c:314 [inline] __kasan_slab_alloc+0x74/0x8c mm/kasan/common.c:340 kasan_slab_alloc include/linux/kasan.h:201 [inline] slab_post_alloc_hook mm/slub.c:3813 [inline] slab_alloc_node mm/slub.c:3860 [inline] kmem_cache_alloc_node+0x204/0x4c0 mm/slub.c:3903 __alloc_skb+0x19c/0x3d8 net/core/skbuff.c:641 alloc_skb include/linux/skbuff.h:1296 [inline] kcm_sendmsg+0x1d3c/0x2124 net/kcm/kcmsock.c:783 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg net/socket.c:745 [inline] sock_sendmsg+0x220/0x2c0 net/socket.c:768 splice_to_socket+0x7cc/0xd58 fs/splice.c:889 do_splice_from fs/splice.c:941 [inline] direct_splice_actor+0xec/0x1d8 fs/splice.c:1164 splice_direct_to_actor+0x438/0xa0c fs/splice.c:1108 do_splice_direct_actor --- truncated---		

CVE Number	Description	Base Score	Reference
CVE-2024-44943	In the Linux kernel, the following vulnerability has been resolved: mm: gup: stop abusing try_grab_folio A kernel warning was reported when pinning folio in CMA memory when launching SEV virtual machine. The splat looks like: [464.325306] WARNING: CPU: 13 PID: 6734 at mm/gup.c:1313 __get_user_pages+0x423/0x520 [464.325464] CPU: 13 PID: 6734 Comm: qemu-kvm Kdump: loaded Not tainted 6.6.33+ #6 [464.325477] RIP: 0010:__get_user_pages+0x423/0x520 [464.325515] Call Trace: [464.325520] <TASK> [464.325523] ? __get_user_pages+0x423/0x520 [464.325528] ? __warn+0x81/0x130 [464.325536] ? __get_user_pages+0x423/0x520 [464.325541] ? report_bug+0x171/0x1a0 [464.325549] ? handle_bug+0x3c/0x70 [464.325554] ? exc_invalid_op+0x17/0x70 [464.325558] ? asm_exc_invalid_op+0x1a/0x20 [464.325567] ? __get_user_pages+0x423/0x520 [464.325575] __gup_longterm_locked+0x212/0x7a0 [464.325583] internal_get_user_pages_fast+0xfb/0x190 [464.325590] pin_user_pages_fast+0x47/0x60 [464.325598] sev_pin_memory+0xca/0x170 [kvm_amd] [464.325616] sev_mem_enc_register_region+0x81/0x130 [kvm_amd] Per the analysis done by yangge, when starting the SEV virtual machine, it will call pin_user_pages_fast(..., FOLL_LONGTERM, ...) to pin the memory. But the page is in CMA area, so fast GUP will fail then fallback to the slow path due to the longterm pinnalbe check in try_grab_folio(). The slow path will try to pin the pages then migrate them out of CMA area. But the slow path also uses try_grab_folio() to pin the page, it will also fail due to the same check then the above warning is triggered. In addition, the try_grab_folio() is supposed to be used in fast path and it elevates folio refcount by using add ref unless zero. We are guaranteed to have at least one stable reference in slow path, so the simple atomic add could be used. The performance difference should be trivial, but the misuse may be confusing and misleading. Redefined try_grab_folio() to try_grab_folio_fast(), and try_grab_page() to try_grab_folio(), and use them in the proper paths. This solves both the abuse and the kernel warning. The proper naming makes their usecase more clear and should prevent from abusing in the future. peterx said: : The user will see the pin fails, for gpu-slow it further triggers the WARN : right below that failure (as in the original report): : : folio = try_grab_folio(page, page_increm - 1, : foll_flags); : if (WARN_ON_ONCE(!folio)) { <---------- here : /* : * Release the 1st page ref if the : * folio is problematic, fail hard. : */ : gup_put_folio(page_folio(page), 1, : foll_flags); : ret = -EFAULT; : goto out; : } [1] https://lore.kernel.org/linux-mm/1719478388-31917-1-git-send-email-yangge1116@126.com/ [shy828301@gmail.com: fix implicit declaration of function try_grab_folio_fast] Link: https://lkml.kernel.org/r/CAHbLzkowMSso-4Nufc9hcMehQsK9PNz3OSu-+eniU-2Mm-xjhA@mail.gmail.com	5.5	More Details
CVE-2024-39612	in OpenHarmony v4.0.0 and prior versions allow a local attacker cause information leak through out-of-bounds Read.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7269	Improper Neutralization of Input During Web Page Generation vulnerability in "Update of Personal Details" form in ConnX ESP HR Management allows Stored XSS attack. An attacker might inject a script to be run in user's browser. After multiple attempts to contact the vendor we did not receive any answer. The finder provided the information that this issue affects ESP HR Management versions before 6.6.	5.4	More Details
CVE-2024-41345	openflights commit 5234b5b is vulnerable to Cross-Site Scripting (XSS) via php/trip.php	5.4	More Details
CVE-2024-43947	Cross-Site Request Forgery (CSRF) vulnerability in Dinesh Karki WP Armour Extended.This issue affects WP Armour Extended: from n/a through 1.26.	5.4	More Details
CVE-2024-45047	svelte performance oriented web framework. A potential mXSS vulnerability exists in Svelte for versions up to but not including 4.2.19. Svelte improperly escapes HTML on server-side rendering. The assumption is that attributes will always stay as such, but in some situation the final DOM tree rendered on browsers is different from what Svelte expects on server-side rendering. This may be leveraged to perform XSS attacks, and a type of the XSS is known as mXSS (mutation XSS). More specifically, this can occur when injecting malicious content into an attribute within a `noscript` tag. This issue has been addressed in release version 4.2.19. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.4	More Details
CVE-2024-41346	openflights commit 5234b5b is vulnerable to Cross-Site Scripting (XSS) via php/submit.php	5.4	More Details
CVE-2024-45046	PHPSpreadsheet is a pure PHP library for reading and writing spreadsheet files. In affected versions `\PhpOffice\PhpSpreadsheet\Writer\Html` doesn't sanitize spreadsheet styling information such as font names, allowing an attacker to inject arbitrary JavaScript on the page. As a result an attacker may used a crafted spreadsheet to fully takeover a session of a user viewing spreadsheet files as HTML. This issue has been addressed in release version 2.1.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	5.4	More Details
CVE-2024-5417	The Gutentor WordPress plugin before 3.3.6 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2024-6585	Multiple stored cross-site scripting (“XSS”) vulnerabilities in the markdown dashboard and dashboard comment functionality of Lightdash version 0.1024.6 allows remote authenticated threat actors to inject malicious scripts into vulnerable web pages. A threat actor could potentially exploit this vulnerability to store malicious JavaScript which executes in the context of a user’s session with the application.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44919	A cross-site scripting (XSS) vulnerability in the component admin_ads.php of SeaCMS v12.9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the ad description parameter.	5.4	More Details
CVE-2024-45528	CodeAstro MembershipM-PHP (aka Membership Management System in PHP) 1.0 allows add_members.php fullname stored XSS.	5.4	More Details
CVE-2024-45313	Overleaf is a web-based collaborative LaTeX editor. When installing Server Pro using the Overleaf Toolkit from before 2024-07-17 or legacy docker-compose.yml from before 2024-08-28, the configuration for LaTeX compiles was insecure by default, requiring the administrator to enable the security features via a configuration setting (`SIBLING_CONTAINERS_ENABLED` in Toolkit, `SANDBOXED_COMPILES` in legacy docker-compose/custom deployments). If these security features are not enabled then users have access to the `sharelatex` container resources (filesystem, network, environment variables) when running compiles, leading to multiple file access vulnerabilities, either directly or via symlinks created during compiles. The setting has now been changed to be secure by default for new installs in the Toolkit and legacy docker-compose deployment. The Overleaf Toolkit has been updated to set `SIBLING_CONTAINERS_ENABLED=true` by default for new installs. It is recommended that any existing installations using the previous default setting migrate to using sibling containers. Existing installations can set `SIBLING_CONTAINERS_ENABLED=true` in `config/overleaf.rc` as a mitigation. In legacy docker-compose/custom deployments `SANDBOXED_COMPILES=true` should be used.	5.4	More Details
CVE-2024-5987	The WP Accessibility Helper (WAH) plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'save_contrast_variations' and 'save_empty_contrast_variations' functions in all versions up to, and including, 0.6.2.8. This makes it possible for authenticated attackers, with Subscriber-level access and above, to edit or delete contrast settings. Please note these issues were patched in 0.6.2.8, though it broke functionality and the vendor has not responded to our follow-ups.	5.4	More Details
CVE-2024-8328	Easy test Online Learning and Testing Platform from HWA JIUH DIGITAL TECHNOLOGY does not properly validate a specific page parameter, allowing remote attackers with regular privilege to inject arbitrary JavaScript code and perform Reflected Cross-site scripting attacks.	5.4	More Details
CVE-2024-45621	The Electron desktop application of Rocket.Chat through 6.3.4 allows stored XSS via links in an uploaded file, related to failure to use a separate browser upon encountering third-party external actions from PDF documents.	5.4	More Details
CVE-2024-45180	SquaredUp DS for SCOM 6.2.1.11104 allows XSS.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3679	The Premium SEO Pack – WP SEO Plugin plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.6.001. This makes it possible for unauthenticated attackers to view limited information from password protected posts through the social meta data.	5.3	More Details
CVE-2024-20286	A vulnerability in the Python interpreter of Cisco NX-OS Software could allow an authenticated, low-privileged, local attacker to escape the Python sandbox and gain unauthorized access to the underlying operating system of the device. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by manipulating specific functions within the Python interpreter. A successful exploit could allow an attacker to escape the Python sandbox and execute arbitrary commands on the underlying operating system with the privileges of the authenticated user. Note: An attacker must be authenticated with Python execution privileges to exploit these vulnerabilities. For more information regarding Python execution privileges, see product-specific documentation, such as the section of the Cisco Nexus 9000 Series NX-OS Programmability Guide.	5.3	More Details
CVE-2024-20285	A vulnerability in the Python interpreter of Cisco NX-OS Software could allow an authenticated, low-privileged, local attacker to escape the Python sandbox and gain unauthorized access to the underlying operating system of the device. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by manipulating specific functions within the Python interpreter. A successful exploit could allow an attacker to escape the Python sandbox and execute arbitrary commands on the underlying operating system with the privileges of the authenticated user. Note: An attacker must be authenticated with Python execution privileges to exploit these vulnerabilities. For more information regarding Python execution privileges, see product-specific documentation, such as the section of the Cisco Nexus 9000 Series NX-OS Programmability Guide.	5.3	More Details
CVE-2024-2541	The Popup Builder plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.3.3 via the Subscribers Import feature. This makes it possible for unauthenticated attackers to extract sensitive data after an administrator has imported subscribers via a CSV file. This data may include the first name, last name, e-mail address, and potentially other personally identifiable information of subscribers.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20284	A vulnerability in the Python interpreter of Cisco NX-OS Software could allow an authenticated, low-privileged, local attacker to escape the Python sandbox and gain unauthorized access to the underlying operating system of the device. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by manipulating specific functions within the Python interpreter. A successful exploit could allow an attacker to escape the Python sandbox and execute arbitrary commands on the underlying operating system with the privileges of the authenticated user. Note: An attacker must be authenticated with Python execution privileges to exploit these vulnerabilities. For more information regarding Python execution privileges, see product-specific documentation, such as the section of the Cisco Nexus 9000 Series NX-OS Programmability Guide.	5.3	More Details
CVE-2024-7447	The Interactive Contact Form and Multi Step Form Builder with Drag & Drop Editor – Funnelforms Free plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'fnsf_af2_handel_file_upload' function in all versions up to, and including, 3.7.3.2. This makes it possible for unauthenticated attackers to upload arbitrary media to the site, even if no forms exist.	5.3	More Details
CVE-2024-7573	The Relevanssi Live Ajax Search plugin for WordPress is vulnerable to argument injection in all versions up to, and including, 2.4. This is due to insufficient validation of input supplied via POST data in the 'search' function. This makes it possible for unauthenticated attackers to inject arbitrary arguments into a WP_Query query and potentially expose sensitive information such as attachments or private posts.	5.3	More Details
CVE-2024-45043	The OpenTelemetry Collector module AWS firehose receiver is for ingesting AWS Kinesis Data Firehose delivery stream messages and parsing the records received based on the configured record type. `awsfirehosereceiver` allows unauthenticated remote requests, even when configured to require a key. OpenTelemetry Collector can be configured to receive CloudWatch metrics via an AWS Firehose Stream. Firehose sets the header `X-Amz-Firehose-Access-Key` with an arbitrary configured string. The OpenTelemetry Collector awsfirehosereceiver can optionally be configured to require this key on incoming requests. However, when this is configured it **still accepts incoming requests with no key**. Only OpenTelemetry Collector users configured with the “alpha” `awsfirehosereceiver` module are affected. This module was added in version v0.49.0 of the “Contrib” distribution (or may be included in custom builds). There is a risk of unauthorized users writing metrics. Carefully crafted metrics could hide other malicious activity. There is no risk of exfiltrating data. It’s likely these endpoints will be exposed to the public internet, as Firehose does not support private HTTP endpoints. A fix was introduced in PR #34847 and released with v0.108.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45312	Overleaf is a web-based collaborative LaTeX editor. Overleaf Community Edition and Server Pro prior to version 5.0.7 (or 4.2.7 for the 4.x series) contain a vulnerability that allows an arbitrary language parameter in client spelling requests to be passed to the `aspell` executable running on the server. This causes `aspell` to attempt to load a dictionary file with an arbitrary filename. File access is limited to the scope of the overleaf server. The problem is patched in versions 5.0.7 and 4.2.7. Previous versions can be upgraded using the Overleaf toolkit `bin/upgrade` command. Users unable to upgrade may block POST requests to `/spelling/check` via a Web Application Firewall will prevent access to the vulnerable spell check feature. However, upgrading is advised.	5.3	More Details
CVE-2024-45232	An issue was discovered in powermail extension through 12.3.5 for TYPO3. It fails to validate the mail parameter of the confirmationAction, resulting in Insecure Direct Object Reference (IDOR). An unauthenticated attacker can use this to display the user-submitted data of all forms persisted by the extension. This can only be exploited when the extension is configured to save submitted form data to the database (plugin.tx_powermail.settings.db.enable=1), which however is the default setting of the extension. The fixed versions are 7.5.0, 8.5.0, 10.9.0, and 12.4.0	5.3	More Details
CVE-2024-8388	Multiple prompts and panels from both Firefox and the Android OS could be used to obscure the notification announcing the transition to fullscreen mode after the fix for CVE-2023-6870 in Firefox 121. This could lead to spoofing the browser UI if the sudden appearance of the prompt distracted the user from noticing the visual transition happening behind the prompt. These notifications now use the Android Toast feature. *This bug only affects Firefox on Android. Other operating systems are unaffected.* This vulnerability affects Firefox < 130.	5.3	More Details
CVE-2024-6551	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 3.15.1. This is due to the plugin utilizing Symfony and leaving display_errors on within test files. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	5.3	More Details
CVE-2024-5857	The Interactive Contact Form and Multi Step Form Builder with Drag & Drop Editor – Funnelforms Free plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the af2_handel_file_remove AJAX action in all versions up to, and including, 3.7.3.2. This makes it possible for unauthenticated attackers to delete arbitrary media files.	5.3	More Details
CVE-2024-6448	The Mollie Payments for WooCommerce plugin for WordPress is vulnerable to information exposure in all versions up to, and including, 7.7.0. This is due to the error reporting being enabled by default in multiple plugin files. This makes it possible for unauthenticated attackers to obtain the full path to instances, which they may be able to use in combination with other vulnerabilities or to simplify reconnaissance work. On its own, this information is of very limited use.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45440	core/authorize.php in Drupal 11.x-dev allows Full Path Disclosure (even when error logging is None) if the value of hash_salt is file_get_contents of a file that does not exist.	5.3	More Details
CVE-2024-38303	Dell PowerEdge Platform, 14G Intel BIOS version(s) prior to 2.22.x, contains an Improper Input Validation vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	5.3	More Details
CVE-2024-8297	A vulnerability was found in kitsada8621 Digital Library Management System 1.0. It has been classified as problematic. Affected is the function JwtRefreshAuth of the file middleware/jwt_refresh_token_middleware.go. The manipulation of the argument Authorization leads to improper output neutralization for logs. It is possible to launch the attack remotely. The name of the patch is 81b3336b4c9240f0bf50c13cb8375cf860d945f1. It is recommended to apply a patch to fix this issue.	5.3	More Details
CVE-2024-8195	The Permalink Manager Lite plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'debug_data', 'debug_query', and 'debug_redirect' functions in all versions up to, and including, 2.4.4. This makes it possible for unauthenticated attackers to extract sensitive data including password, title, and content of password-protected posts.	5.3	More Details
CVE-2022-4100	The WP Cerber Security plugin for WordPress is vulnerable to IP Protection bypass in versions up to, and including 9.4 due to the plugin improperly checking for a visitor's IP address. This makes it possible for an attacker whose IP address has been blocked to bypass this control by setting the X-Forwarded-For: HTTP header to an IP Address that hasn't been blocked.	5.3	More Details
CVE-2024-45304	Cairo-Contracts are OpenZeppelin Contracts written in Cairo for Starknet, a decentralized ZK Rollup. This vulnerability can lead to unauthorized ownership transfer, contrary to the original owner's intention of leaving the contract without an owner. It introduces a security risk where an unintended party (pending owner) can gain control of the contract after the original owner has renounced ownership. This could also be used by a malicious owner to simulate leaving a contract without an owner, to later regain ownership by previously having proposed himself as a pending owner. This issue has been addressed in release version 0.16.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2022-4539	The Web Application Firewall plugin for WordPress is vulnerable to IP Address Spoofing in versions up to, and including, 2.1.2. This is due to insufficient restrictions on where the IP Address information is being retrieved for request logging and login restrictions. Attackers can supply the X-Forwarded-For header with with a different IP Address that will be logged and can be used to bypass settings that may have blocked out an IP address or country from logging in.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4536	The IP Vault – WP Firewall plugin for WordPress is vulnerable to IP Address Spoofing in versions up to, and including, 1.1. This is due to insufficient restrictions on where the IP Address information is being retrieved for request logging and login restrictions. Attackers can supply the X-Forwarded-For header with with a different IP Address that will be logged and can be used to bypass settings that may have blocked out an IP address or country from logging in.	5.3	More Details
CVE-2021-38120	A vulnerability identified in Advance Authentication that allows bash command Injection in administrative controlled functionality of backup due to improper handling in provided command parameters. This issue affects NetIQ Advance Authentication version before 6.3.5.1.	5.1	More Details
CVE-2024-34463	BPL Personal Weighing Scale PWS-01BT IND/09/18/599 devices send sensitive information in unencrypted BLE packets. (The packet data also lacks authentication and integrity protection.)	5.1	More Details
CVE-2024-6343	A buffer overflow vulnerability in the CGI program of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device.	4.9	More Details
CVE-2024-43803	The Bare Metal Operator (BMO) implements a Kubernetes API for managing bare metal hosts in Metal3. The `BareMetalHost` (BMH) CRD allows the `userData`, `metaData`, and `networkData` for the provisioned host to be specified as links to Kubernetes Secrets. There are fields for both the `Name` and `Namespace` of the Secret, meaning that versions of the baremetal-operator prior to 0.8.0, 0.6.2, and 0.5.2 will read a `Secret` from any namespace. A user with access to create or edit a `BareMetalHost` can thus exfiltrate a `Secret` from another namespace by using it as e.g. the `userData` for provisioning some host (note that this need not be a real host, it could be a VM somewhere). BMO will only read a key with the name `value` (or `userData`, `metaData`, or `networkData`), so that limits the exposure somewhat. `value` is probably a pretty common key though. Secrets used by _other_ `BareMetalHost`s in different namespaces are always vulnerable. It is probably relatively unusual for anyone other than cluster administrators to have RBAC access to create/edit a `BareMetalHost`. This vulnerability is only meaningful, if the cluster has users other than administrators and users' privileges are limited to their respective namespaces. The patch prevents BMO from accepting links to Secrets from other namespaces as BMH input. Any BMH configuration is only read from the same namespace only. The problem is patched in BMO releases v0.7.0, v0.6.2 and v0.5.2 and users should upgrade to those versions. Prior upgrading, duplicate the BMC Secrets to the namespace where the corresponding BMH is. After upgrade, remove the old Secrets. As a workaround, an operator can configure BMO RBAC to be namespace scoped for Secrets, instead of cluster scoped, to prevent BMO from accessing Secrets from other namespaces.	4.9	More Details
CVE-2024-42901	A CSV injection vulnerability in Lime Survey v6.5.12 allows attackers to execute arbitrary code via uploading a crafted CSV file.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6927	The Viral Signup WordPress plugin through 2.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-43922	Improper Control of Generation of Code ('Code Injection') vulnerability in NitroPack Inc. NitroPack allows Code Injection.This issue affects NitroPack: from n/a through 1.16.7.	4.8	More Details
CVE-2024-7132	The Page Builder Gutenberg Blocks WordPress plugin before 3.1.13 does not escape the content of post embed via one of its block, which could allow users with the capability to publish posts (editor and admin by default) to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-8399	Websites could utilize Javascript links to spoof URL addresses in the Focus navigation bar This vulnerability affects Focus for iOS < 130.	4.7	More Details
CVE-2024-8304	A vulnerability has been found in jpress up to 5.1.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/template/edit of the component Template Module Handler. The manipulation leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2024-35118	IBM MaaS360 for Android 6.31 through 8.60 is using hard coded credentials that can be obtained by a user with physical access to the device.	4.6	More Details
CVE-2024-43801	Jellyfin is an open source self hosted media server. The Jellyfin user profile image upload accepts SVG files, allowing for a stored XSS attack against an admin user via a specially crafted malicious SVG file. When viewed by an admin outside of the Jellyfin Web UI (e.g. via "view image" in a browser), this malicious SVG file could interact with the browser's LocalStorage and retrieve an AccessToken, which in turn can be used in an API call to elevate the target user to a Jellyfin administrator. The actual attack vector is unlikely to be exploited, as it requires specific actions by the administrator to view the SVG image outside of Jellyfin's WebUI, i.e. it is not a passive attack. The underlying exploit mechanism is solved by PR #12490, which forces attached images (including the potential malicious SVG) to be treated as attachments and thus downloaded by browsers, rather than viewed. This prevents exploitation of the LocalStorage of the browser. This PR has been merged and the relevant code changes are included in release version 10.9.10. All users are advised to upgrade.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43412	Xibo is an open source digital signage platform with a web content management system (CMS). Prior to version 4.1.0, a cross-site scripting vulnerability in Xibo CMS allows authorized users to execute arbitrary JavaScript via the file preview function. Users can upload HTML/CSS/JS files into the Xibo Library via the Generic File module to be referenced on Displays and in Layouts. This is intended functionality. When previewing these resources from the Library and Layout editor they are executed in the users browser. This will be disabled in future releases, and users are encouraged to use the new developer tools in 4.1 to design their widgets which require this type of functionality. This behavior has been changed in 4.1.0 to preview previewing of generic files. There are no workarounds for this issue.	4.6	More Details
CVE-2024-45306	Vim is an open source, command line text editor. Patch v9.1.0038 optimized how the cursor position is calculated and removed a loop, that verified that the cursor position always points inside a line and does not become invalid by pointing beyond the end of a line. Back then we assumed this loop is unnecessary. However, this change made it possible that the cursor position stays invalid and points beyond the end of a line, which would eventually cause a heap-buffer-overflow when trying to access the line pointer at the specified cursor position. It's not quite clear yet, what can lead to this situation that the cursor points to an invalid position. That's why patch v9.1.0707 does not include a test case. The only observed impact has been a program crash. This issue has been addressed in with the patch v9.1.0707. All users are advised to upgrade.	4.5	More Details
CVE-2024-20289	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, low-privileged, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments for a specific CLI command. An attacker could exploit this vulnerability by including crafted input as the argument of the affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user.	4.4	More Details
CVE-2024-0110	NVIDIA CUDA Toolkit contains a vulnerability in command `cuobjdump` where a user may cause an out-of-bound write by passing in a malformed ELF file. A successful exploit of this vulnerability may lead to code execution or denial of service.	4.4	More Details
CVE-2023-7256	In affected libpcap versions during the setup of a remote packet capture the internal function sock_initaddress() calls getaddrinfo() and possibly freeaddrinfo(), but does not clearly indicate to the caller function whether freeaddrinfo() still remains to be called after the function returns. This makes it possible in some scenarios that both the function and its caller call freeaddrinfo() for the same allocated memory block. A similar problem was reported in Apple libpcap, to which Apple assigned CVE-2023-40400.	4.4	More Details
CVE-2024-0111	NVIDIA CUDA Toolkit contains a vulnerability in command 'cuobjdump' where a user may cause a crash or produce incorrect output by passing a malformed ELF file. A successful exploit of this vulnerability may lead to a limited denial of service or data tampering.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3944	The WP To Do plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment in all versions up to, and including, 1.3.0 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.	4.4	More Details
CVE-2024-20085	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560.	4.4	More Details
CVE-2024-8006	Remote packet capture support is disabled by default in libpcap. When a user builds libpcap with remote packet capture support enabled, one of the functions that become available is pcap_findalldevs_ex(). One of the function arguments can be a filesystem path, which normally means a directory with input data files. When the specified path cannot be used as a directory, the function receives NULL from opendir(), but does not check the return value and passes the NULL value to readdir(), which causes a NULL pointer derefence.	4.4	More Details
CVE-2024-20088	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543.	4.4	More Details
CVE-2024-20084	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561.	4.4	More Details
CVE-2024-8334	A vulnerability was found in master-nan Sweet-CMS up to 5f441e022b8876f07cde709c77b5be6d2f262e3f. It has been rated as problematic. This issue affects the function LogHandler of the file middleware/log.go. The manipulation leads to improper output neutralization for logs. The attack may be initiated remotely. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The identifier of the patch is 2024c370e6c78b07b358c9d4257fa5d1be732c38. It is recommended to apply a patch to fix this issue.	4.3	More Details
CVE-2020-36830	A vulnerability was found in nescalante urlregex up to 0.5.0 and classified as problematic. This issue affects some unknown processing of the file index.js of the component Backtracking. The manipulation leads to inefficient regular expression complexity. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 0.5.1 is able to address this issue. The identifier of the patch is e5a085afe6abfaea1d1a78f54c45af9ef43ca1f9. It is recommended to upgrade the affected component.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41564	EMI v.1.1.10 and before, fixed in v.1.1.11, contains an Improper Validation of Specified Index, Position, or Offset in Input vulnerability. The specific issue is a failure to validate slot index and decrement stack count in EMI mod for Minecraft, which allows in-game item duplication.	4.3	More Details
CVE-2024-45619	A vulnerability was found in OpenSC, OpenSC tools, PKCS#11 module, minidriver, and CTK. An attacker could use a crafted USB Device or Smart Card, which would present the system with a specially crafted response to APDUs. When buffers are partially filled with data, initialized parts of the buffer can be incorrectly accessed.	4.3	More Details
CVE-2024-6053	Improper access control in the clipboard synchronization feature in TeamViewer Full Client prior version 15.57 and TeamViewer Meeting prior version 15.55.3 can lead to unintentional sharing of the clipboard with the current presenter of a meeting.	4.3	More Details
CVE-2024-7690	The DN Popup WordPress plugin through 1.2.2 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	4.3	More Details
CVE-2024-20279	A vulnerability in the restricted security domain implementation of Cisco Application Policy Infrastructure Controller (APIC) could allow an authenticated, remote attacker to modify the behavior of default system policies, such as quality of service (QoS) policies, on an affected system. This vulnerability is due to improper access control when restricted security domains are used to implement multi-tenancy. An attacker with a valid user account associated with a restricted security domain could exploit this vulnerability. A successful exploit could allow the attacker to read, modify, or delete child policies created under default system policies, which are implicitly used by all tenants in the fabric, resulting in disruption of network traffic. Exploitation is not possible for policies under tenants that an attacker has no authorization to access.	4.3	More Details
CVE-2024-45270	WordPress plugin "Carousel Slider" provided by Sayful Islam contains a cross-site request forgery vulnerability on Hero image selection feature. While logged in to the WordPress site with Carousel Slider plugin enabled, accessing a crafted page may cause a user to alter the contents of the WordPress site.	4.3	More Details
CVE-2024-45269	WordPress plugin "Carousel Slider" provided by Sayful Islam contains a cross-site request forgery vulnerability on Carousel image selection feature. While logged in to the WordPress site with Carousel Slider plugin enabled, accessing a crafted page may cause a user to alter the contents of the WordPress site.	4.3	More Details
CVE-2024-8366	A vulnerability was found in code-projects Pharmacy Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /index.php?id=userProfileEdit of the component Update My Profile Page. The manipulation of the argument fname/lname/email with the input <script>alert(1) </script> leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41434	PingCAP TiDB v8.1.0 was discovered to contain a buffer overflow via the component (*Column).GetDecimal. This allows attackers to cause a Denial of Service (DoS) via a crafted input to the 'RemoveUnnecessaryFirstRow', it will check the expression between 'Agg' and 'GroupBy', but does not check the return type. NOTE: PingCAP disputes this, arguing that reproduction did not cause the security impact of service interruption to other users. They maintain it is a complex query bug in the product but not a DoS.	4.3	More Details
CVE-2024-21658	discourse-calendar is a discourse plugin which adds the ability to create a dynamic calendar in the first post of a topic. The limit on region value length is too generous. This allows a malicious actor to cause a Discourse instance to use excessive bandwidth and disk space. This issue has been patched in main the main branch. There are no workarounds for this vulnerability. Please upgrade as soon as possible.	4.3	More Details
CVE-2024-8319	The Tourfic plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.11.20. This is due to missing or incorrect nonce validation on the tf_order_status_email_resend_function, tf_visitor_details_edit_function, tf_checkinout_details_edit_function, tf_order_status_edit_function, tf_order_bulk_action_edit_function, tf_remove_room_order_ids, and tf_delete_old_review_fields functions. This makes it possible for unauthenticated attackers to resend order status emails, update visitor/order details, edit check-in/out details, edit order status, perform bulk order status updates, remove room order IDs, and delete old review fields, respectively, via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2024-42698	Roughly Enough Items (REI) v.16.0.729 and before contains an Improper Validation of Specified Index, Position, or Offset in Input vulnerability. The specific issue is a failure to validate slot index and decrement stack count in the Roughly Enough Items (REI) mod for Minecraft, which allows in-game item duplication.	4.3	More Details
CVE-2024-41565	JustEnoughItems (JEI) 19.5.0.33 and before contains an Improper Validation of Specified Index, Position, or Offset in Input vulnerability. The specific issue is a failure to validate slot index in JEI for Minecraft, which allows in-game item duplication.	4.3	More Details
CVE-2024-7418	The The Post Grid – Shortcode, Gutenberg Blocks and Elementor Addon for Post Grid plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 7.7.11 via the post_query_guten and post_query functions. This makes it possible for authenticated attackers, with contributor-level access and above, to extract information from posts that are not public (i.e. draft, future, etc..).	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5053	The Contact Form Plugin by Fluent Forms for Quiz, Survey, and Drag & Drop WP Form Builder plugin for WordPress is vulnerable to unauthorized Malichimp API key update due to an insufficient capability check on the verifyRequest function in all versions up to, and including, 5.1.18. This makes it possible for Form Managers with a Subscriber-level access and above to modify the Mailchimp API key used for integration. At the same time, missing Mailchimp API key validation allows the redirect of the integration requests to the attacker-controlled server.	4.2	More Details
CVE-2024-45678	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected.	4.2	More Details
CVE-2024-1543	The side-channel protected T-Table implementation in wolfSSL up to version 5.6.5 protects against a side-channel attacker with cache-line resolution. In a controlled environment such as Intel SGX, an attacker can gain a per instruction sub-cache-line resolution allowing them to break the cache-line-level protection. For details on the attack refer to: https://doi.org/10.46586/tches.v2024.i1.457-500	4.1	More Details
CVE-2024-45616	A vulnerability was found in OpenSC, OpenSC tools, PKCS#11 module, minidriver, and CTK. An attacker could use a crafted USB Device or Smart Card, which would present the system with a specially crafted response to APDUs. The following problems were caused by insufficient control of the response APDU buffer and its length when communicating with the card.	3.9	More Details
CVE-2024-45617	A vulnerability was found in OpenSC, OpenSC tools, PKCS#11 module, minidriver, and CTK. An attacker could use a crafted USB Device or Smart Card, which would present the system with a specially crafted response to APDUs. Insufficient or missing checking of return values of functions leads to unexpected work with variables that have not been initialized.	3.9	More Details
CVE-2024-45615	A vulnerability was found in OpenSC, OpenSC tools, PKCS#11 module, minidriver, and CTK. The problem is missing initialization of variables expected to be initialized (as arguments to other functions, etc.).	3.9	More Details
CVE-2024-45618	A vulnerability was found in pkcs15-init in OpenSC. An attacker could use a crafted USB Device or Smart Card, which would present the system with a specially crafted response to APDUs. Insufficient or missing checking of return values of functions leads to unexpected work with variables that have not been initialized.	3.9	More Details
CVE-2024-45620	A vulnerability was found in the pkcs15-init tool in OpenSC. An attacker could use a crafted USB Device or Smart Card, which would present the system with a specially crafted response to APDUs. When buffers are partially filled with data, initialized parts of the buffer can be incorrectly accessed.	3.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38304	Dell PowerEdge Platform, 14G Intel BIOS version(s) prior to 2.22.x, contains an Access of Memory Location After End of Buffer vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	3.8	More Details
CVE-2024-39300	Missing authentication vulnerability exists in Telnet function of WAB-I1750-PS v1.5.10 and earlier. When Telnet function of the product is enabled, a remote attacker may login to the product without authentication and alter the product's settings.	3.7	More Details
CVE-2024-43944	Incorrect Authorization vulnerability in Yassine Idrissi Maintenance & Coming Soon Redirect Animation allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Maintenance & Coming Soon Redirect Animation: from n/a through 2.1.3.	3.7	More Details
CVE-2024-45310	runc is a CLI tool for spawning and running containers according to the OCI specification. runc 1.1.13 and earlier, as well as 1.2.0-rc2 and earlier, can be tricked into creating empty files or directories in arbitrary locations in the host filesystem by sharing a volume between two containers and exploiting a race with `os.MkdirAll`. While this could be used to create empty files, existing files would not be truncated. An attacker must have the ability to start containers using some kind of custom volume configuration. Containers using user namespaces are still affected, but the scope of places an attacker can create inodes can be significantly reduced. Sufficiently strict LSM policies (SELinux/Apparmor) can also in principle block this attack -- we suspect the industry standard SELinux policy may restrict this attack's scope but the exact scope of protection hasn't been analysed. This is exploitable using runc directly as well as through Docker and Kubernetes. The issue is fixed in runc v1.1.14 and v1.2.0-rc3. Some workarounds are available. Using user namespaces restricts this attack fairly significantly such that the attacker can only create inodes in directories that the remapped root user/group has write access to. Unless the root user is remapped to an actual user on the host (such as with rootless containers that don't use `/etc/sub[ug]id`), this in practice means that an attacker would only be able to create inodes in world-writable directories. A strict enough SELinux or AppArmor policy could in principle also restrict the scope if a specific label is applied to the runc runtime, though neither the extent to which the standard existing policies block this attack nor what exact policies are needed to sufficiently restrict this attack have been thoroughly tested.	3.6	More Details
CVE-2024-8337	A vulnerability, which was classified as problematic, has been found in SourceCodester Contact Manager with Export to VCF 1.0. Affected by this issue is some unknown functionality of the file index.html. The manipulation of the argument contact_name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8370	A vulnerability classified as problematic was found in Grocy up to 4.2.0. This vulnerability affects unknown code of the file /api/files/recipepictures/ of the component SVG File Upload Handler. The manipulation of the argument force_serve_as with the input picture' leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. Unfortunately, the project maintainer does not want to be quoted in any way regarding the dispute rationale. The security policy of the project implies that this finding is "practically irrelevant" due to authentication requirements.	3.5	More Details
CVE-2024-43413	Xibo is an open source digital signage platform with a web content management system (CMS). Prior to version 4.1.0, a cross-site scripting vulnerability in Xibo CMS allows authorized users to execute JavaScript via the DataSet functionality. Users can design a DataSet with a HTML column which contains JavaScript, which is intended functionality. The JavaScript gets executed on the Data Entry page and in any Layouts which reference it. This behavior has been changed in 4.1.0 to show HTML/CSS/JS as code on the Data Entry page. There are no workarounds for this issue.	3.5	More Details
CVE-2024-44918	A cross-site scripting (XSS) vulnerability in the component admin_datarelate.php of SeaCMS v12.9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	3.5	More Details
CVE-2024-8367	A vulnerability was found in HM Courts & Tribunals Service Probate Back Office up to c1afe0cdb2b2766d9e24872c4e827f8b82a6cd31. It has been classified as problematic. Affected is an unknown function of the file src/main/java/uk/gov/hmcts/probate/service/NotificationService.java of the component Markdown Handler. The manipulation leads to injection. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The patch is identified as d90230d7cf575e5b0852d56660104c8bd2503c34. It is recommended to apply a patch to fix this issue.	3.5	More Details
CVE-2024-0109	NVIDIA CUDA Toolkit contains a vulnerability in command `cuobjdump` where a user may cause a crash by passing in a malformed ELF file. A successful exploit of this vulnerability may cause an out of bounds read in the unprivileged process memory which could lead to a limited denial of service.	3.3	More Details
CVE-2024-28044	in OpenHarmony v4.1.0 and prior versions allow a local attacker cause crash through integer overflow.	3.3	More Details
CVE-2024-45054	Hwameistor is an HA local storage system for cloud-native stateful workloads. This ClusterRole has * verbs of * resources. If a malicious user can access the worker node which has hwameistor's deployment, he/she can abuse these excessive permissions to do whatever he/she likes to the whole cluster, resulting in a cluster-level privilege escalation. This issue has been patched in version 0.14.6. All users are advised to upgrade. Users unable to upgrade should update and limit the ClusterRole using security-role.	2.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-7279	A vulnerability has been found in Secure Systems Engineering Connaisseur up to 3.3.0 and classified as problematic. This vulnerability affects unknown code of the file connaisseur/res/targets_schema.json of the component Delegation Name Handler. The manipulation leads to inefficient regular expression complexity. The complexity of an attack is rather high. The exploitation appears to be difficult. Upgrading to version 3.3.1 is able to address this issue. The name of the patch is 524b73ff7306707f6d3a4d1e86401479bca91b02. It is recommended to upgrade the affected component.	2.6	More Details
CVE-2024-45305	gix-path is a crate of the gitoxide project dealing with git paths and their conversions. `gix-path` executes `git` to find the path of a configuration file that belongs to the `git` installation itself, but mistakenly treats the local repository's configuration as system-wide if no higher scoped configuration is found. In rare cases, this causes a less trusted repository to be treated as more trusted, or leaks sensitive information from one repository to another, such as sending credentials to another repository's remote. In `gix_path::env`, the underlying implementation of the `installation_config` and `installation_config_prefix` functions calls `git config -l --show-origin` and parses the first line of the output to extract the path to the configuration file holding the configuration variable of highest scope. It is believed to be very difficult to exploit this vulnerability deliberately, due to the need either to anticipate a situation in which higher-scoped configuration variables would be absent, or to arrange for this to happen. Although any operating system may be affected, users running Apple Git on macOS are much less likely to be affected. This issue has been addressed in release version 0.10.10. All users are advised to upgrade.	2.5	More Details
CVE-2024-2502	An application can be configured to block boot attempts after consecutive tamper resets are detected, which may not occur as expected. This is possible because the TAMPERRSTCAUSE register may not be properly updated when a level 4 tamper event (a tamper reset) occurs. This impacts Series 2 HSE-SVH devices, including xG23B, xG24B, xG25B, and xG28B, but does not impact xG21B. To mitigate this issue, upgrade to SE Firmware version 2.2.6 or later.	2.0	More Details
CVE-2022-4424	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error and is not a valid vulnerability. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-7619	Rejected reason: Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that there was not reasonable evidence to determine the existence of a vulnerability.	N/A	More Details
CVE-2022-4530	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error and is not a valid vulnerability. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4540	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error and is not a valid vulnerability. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-42379	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-7051	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2022-4412	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error and is not a valid vulnerability. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2022-4528	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error and is not a valid vulnerability. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2022-4538	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error and is not a valid vulnerability. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-8371	Rejected reason: Duplicate of CVE-2024-45305.	N/A	More Details
CVE-2024-41718	Rejected reason: ** REJECT ** DO NOT USE THIS CVE ID. ConsultIDs: CVE-2024-39771. Reason: This CVE ID is a reservation duplicate of CVE-2024-39771. Notes: All CVE users should reference CVE-2024-39771 instead of this CVE ID. All references and descriptions in this CVE ID have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-8333	Rejected reason: Test CVE	N/A	More Details
CVE-2024-7712	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-8064	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details