SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 14 August 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-2024-42479	llama.cpp provides LLM inference in C/C++. The unsafe `data` pointer member in the `rpc_tensor` structure can cause arbitrary address writing. This vulnerability is fixed in b3561.	10.0	More Details
CVE-2024-43160	Unrestricted Upload of File with Dangerous Type vulnerability in BerqWP allows Code Injection.This issue affects BerqWP: from n/a through 1.7.6.	10.0	More Details
CVE-2024-42489	Pro Macros provides XWiki rendering macros. Missing escaping in the Viewpdf macro allows any user with view right on the `CKEditor.HTMLConverter` page or edit or comment right on any page to perform remote code execution. Other macros like Viewppt are vulnerable to the same kind of attack. This vulnerability is fixed in 1.10.1.	10.0	More Details
CVE-2024-39791	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code.	10.0	More Details
CVE-2024-42467	openHAB, a provider of open-source home automation software, has add-ons including the visualization add-on CometVisu. Prior to version 4.2.1, the proxy endpoint of openHAB's CometVisu add-on can be accessed without authentication. This proxy-feature can be exploited as Server-Side Request Forgery (SSRF) to induce GET HTTP requests to internal-only servers, in case openHAB is exposed in a non-private network. Furthermore, this proxy-feature can also be exploited as a Cross-Site Scripting (XSS) vulnerability, as an attacker is able to re-route a request to their server and return a page with malicious JavaScript code. Since the browser receives this data directly from the openHAB CometVisu UI, this JavaScript code will be executed with the origin of the CometVisu UI. This allows an attacker to exploit call endpoints on an openHAB server even if the openHAB server is located in a private network. (e.g. by sending an openHAB admin a link that proxies malicious JavaScript.) This issue may lead up to Remote Code Execution (RCE) when chained with other vulnerabilities. Users should upgrade to version 4.2.1 of the CometVisu add-on of openHAB to receive a patch.	10.0	More Details
CVE-2024-22116	An administrator with restricted permissions can exploit the script execution functionality within the Monitoring Hosts section. The lack of default escaping for script parameters enabled this user ability to execute arbitrary code via the Ping script, thereby compromising infrastructure.	9.9	More Details
CVE-2024-42547	TOTOLINK A3100R V4.1.2cu.5050_B20200504 has a buffer overflow vulnerability in the http_host parameter in the loginauth function.	9.8	More Details
CVE-2024-34479	SourceCodester Computer Laboratory Management System 1.0 allows classes/Master.php id SQL Injection.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38530	The Open eClass platform (formerly known as GUnet eClass) is a complete Course Management System. An arbitrary file upload vulnerability in the "save" functionality of the H5P module enables unauthenticated users to upload arbitrary files on the server's filesystem. This may lead in unrestricted RCE on the backend server, since the upload location is accessible from the internet. This vulnerability is fixed in 3.16.	9.8	More Details
CVE-2024-42520	TOTOLINK A3002R v4.0.0-B20230531.1404 contains a buffer overflow vulnerability in /bin/boa via formParentControl.	9.8	More Details
CVE-2024-6917	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Veribilim Software Veribase Order Management allows OS Command Injection.This issue affects Veribase Order Management: before v4.010.2.	9.8	More Details
CVE-2023-7249	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in OpenText OpenText Directory Services allows Path Traversal.This issue affects OpenText Directory Services: from 16.4.2 before 24.1.	9.8	More Details
CVE-2024-42543	TOTOLINK A3700R v9.1.2u.5822_B20200513 has a buffer overflow vulnerability in the http_host parameter in the loginauth function.	9.8	More Details
CVE-2024-42545	TOTOLINK A3700R v9.1.2u.5822_B20200513 has a buffer overflow vulnerability in the ssid parameter in setWizardCfg function.	9.8	More Details
CVE-2024-42546	TOTOLINK A3100R V4.1.2cu.5050_B20200504 has a buffer overflow vulnerability in the password parameter in the loginauth function.	9.8	More Details
CVE-2024-36130	An insufficient authorization vulnerability in web component of EPMM prior to 12.1.0.1 allows an unauthorized attacker within the network to execute arbitrary commands on the underlying operating system of the appliance.	9.8	More Details
CVE-2024-43360	ZoneMinder is a free, open source closed-circuit television software application. ZoneMinder is affected by a time-based SQL Injection vulnerability. This vulnerability is fixed in 1.36.34 and 1.37.61.	9.8	More Details
CVE-2024-7094	The JS Help Desk – The Ultimate Help Desk & Support Plugin plugin for WordPress is vulnerable to PHP Code Injection leading to Remote Code Execution in all versions up to, and including, 2.8.6 via the 'storeTheme' function. This is due to a lack of sanitization on user-supplied values, which replace values in the style.php file, along with missing capability checks. This makes it possible for unauthenticated attackers to execute code on the server. This issue was partially patched in 2.8.6 when the code injection issue was resolved, and fully patched in 2.8.7 when the missing authorization and cross-site request forgery protection was added.	9.8	More Details
CVE-2024-41730	In SAP BusinessObjects Business Intelligence Platform, if Single Signed On is enabled on Enterprise authentication, an unauthorized user can get a logon token using a REST endpoint. The attacker can fully compromise the system resulting in High impact on confidentiality, integrity and availability.	9.8	More Details
CVE-2024-43141	Deserialization of Untrusted Data vulnerability in Roland Barker, xnau webdesign Participants Database allows Object Injection.This issue affects Participants Database: from n/a through 2.5.9.2.	9.8	More Details
CVE-2024-43153	Improper Privilege Management vulnerability in WofficeIO Woffice allows Privilege Escalation.This issue affects Woffice: from n/a through 5.4.10.	9.8	More Details
CVE-2024-41623	An issue in D3D Security D3D IP Camera (D8801) v.V9.1.17.1.4-20180428 allows a local attacker to execute arbitrary code via a crafted payload	9.8	More Details
CVE-2024-7746	Use of Default Credentials vulnerability in Tananaev Solutions Traccar Server on Administrator Panel modules allows Authentication Abuse.This issue affects the privileged transactions implemented by the Traccar solution that should otherwise be protected by the authentication mechanism. These transactions could have an impact on any sensitive aspect of the platform, including Confidentiality, Integrity and Availability.	9.8	More Details
CVE-2024-38063	Windows TCP/IP Remote Code Execution Vulnerability	9.8	More Details
CVE-2024-38140	Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution Vulnerability	9.8	More Details
CVE-2024-38199	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability	9.8	More Details
CVE-2024-7593	Incorrect implementation of an authentication algorithm in Ivanti vTM other than versions 22.2R1 or 22.7R2 allows a remote unauthenticated attacker to bypass authentication of the admin panel.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42469	openHAB, a provider of open-source home automation software, has add-ons including the visualization add-on CometVisu. Prior to version 4.2.1, CometVisu's file system endpoints don't require authentication and additionally the endpoint to update an existing file is susceptible to path traversal. This makes it possible for an attacker to overwrite existing files on the openHAB instance. If the overwritten file is a shell script that is executed at a later time, this vulnerability can allow remote code execution by an attacker. Users should upgrade to version 4.2.1 to receive a patch.	9.8	More Details
CVE-2024-7503	The WooCommerce - Social Login plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.7.5. This is due to the use of loose comparison of the activation code in the 'woo_slg_confirm_email_user' function. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the userID. This requires the email module to be enabled.	9.8	More Details
CVE-2024-28986	SolarWinds Web Help Desk was found to be susceptible to a Java Deserialization Remote Code Execution vulnerability that, if exploited, would allow an attacker to run commands on the host machine. While it was reported as an unauthenticated vulnerability, SolarWinds has been unable to reproduce it without authentication after thorough testing. However, out of an abundance of caution, we recommend all Web Help Desk customers apply the patch, which is now available.	9.8	More Details
CVE-2024-34480	SourceCodester Computer Laboratory Management System 1.0 allows admin/category/view_category.php id SQL Injection.	9.8	More Details
CVE-2024-7350	The Appointment Booking Calendar Plugin and Online Scheduling Plugin – BookingPress plugin for WordPress is vulnerable to authentication bypass in versions 1.1.6 to 1.1.7. This is due to the plugin not properly verifying a user's identity prior to logging them in when completing a booking. This makes it possible for unauthenticated attackers to log in as registered users, including administrators, if they have access to that user's email. This is only exploitable when the 'Auto login user after successful booking' setting is enabled.	9.8	More Details
CVE-2024-42256	In the Linux kernel, the following vulnerability has been resolved: cifs: Fix server re-repick on subrequest retry When a subrequest is marked for needing retry, netfs will call cifs_prepare_write() which will make cifs repick the server for the op before renegotiating credits; it then calls cifs_issue_write() which invokes smb2_async_writev() - which re-repicks the server. If a different server is then selected, this causes the increment of server->in_flight to happen against one record and the decrement to happen against another, leading to misaccounting. Fix this by just removing the repick code in smb2_async_writev(). As this is only called from netfslib-driven code, cifs_prepare_write() should always have been called first, and so server should never be NULL and the preparatory step is repeated in the event that we do a retry. The problem manifests as a warning looking something like: WARNING: CPU: 4 PID: 72896 at fs/smb/client/smb2ops.c:97 smb2_add_credits+0x3f0/0x9e0 [cifs] ... RIP: 0010:smb2_add_credits+0x3f0/0x9e0 [cifs] ... smb2_writev_callback+0x334/0x560 [cifs] cifs_demultiplex_thread+0x77a/0x11b0 [cifs] kthread+0x187/0x1d0 ret_from_fork+0x34/0x60 ret_from_fork_asm+0x1a/0x30 Which may be triggered by a number of different xfstests running against an Azure server in multichannel mode. generic/249 seems the most repeatable, but generic/215, generic/249 and generic/308 may also show it.	9.8	More Details
CVE-2024-7490	Improper Input Validation vulnerability in Microchip Techology Advanced Software Framework example DHCP server can cause remote code execution through a buffer overflow. This vulnerability is associated with program files tinydhcpserver.C and program routines lwip_dhcp_find_option. This issue affects Advanced Software Framework: through 3.52.0.2574. ASF is no longer being supported. Apply provided workaround or migrate to an actively maintained framework.	9.8	More Details
CVE-2024-20454	Multiple vulnerabilities in the web-based management interface of Cisco Small Business SPA300 Series IP Phones and Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system with root privileges. These vulnerabilities exist because incoming HTTP packets are not properly checked for errors, which could result in a buffer overflow. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to overflow an internal buffer and execute arbitrary commands at the root privilege level.	9.8	More Details
CVE-2024-21878	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in Enphase IQ Gateway (formerly known as Envoy) allows OS Command Injection. This vulnerability is present in an internal script.This issue affects Envoy: from 4.x up to and including 8.x and is currently unpatched.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20450	Multiple vulnerabilities in the web-based management interface of Cisco Small Business SPA300 Series IP Phones and Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system with root privileges. These vulnerabilities exist because incoming HTTP packets are not properly checked for errors, which could result in a buffer overflow. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to overflow an internal buffer and execute arbitrary commands at the root privilege level.	9.8	More Details
CVE-2024-41237	A SQL injection vulnerability in /smsa/teacher_login.php in Kashipara Responsive School Management System v1.0 allows an attacker to execute arbitrary SQL commands via the "username" parameter.	9.8	More Details
CVE-2024-38989	izatop bunt v0.29.19 was discovered to contain a prototype pollution via the component /esm/qs.js. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	9.8	More Details
CVE-2024-41912	A vulnerability was discovered in the firmware builds up to 10.10.2.2 in Poly Clariti Manager devices. The firmware flaw does not properly implement access controls.	9.8	More Details
CVE-2024-40472	Sourcecodester Daily Calories Monitoring Tool v1.0 is vulnerable to SQL Injection via "delete-calorie.php."	9.8	More Details
CVE-2024-40477	A SQL injection vulnerability in "/oahms/admin/forgot-password.php" in PHPGurukul Old Age Home Management System v1.0 allows an attacker to execute arbitrary SQL commands via the "email" parameter.	9.8	More Details
CVE-2024-40480	A Broken Access Control vulnerability was found in /admin/update.php and /admin/dashboard.php in Kashipara Online Exam System v1.0, which allows remote unauthenticated attackers to view administrator dashboard and delete valid user accounts via the direct URL access.	9.8	More Details
CVE-2024-40482	An Unrestricted file upload vulnerability was found in "/Membership/edit_member.php" of Kashipara Live Membership System v1.0, which allows attackers to execute arbitrary code via uploading a crafted PHP file.	9.8	More Details
CVE-2024-40486	A SQL injection vulnerability in "/index.php" of Kashipara Live Membership System v1.0 allows remote attackers to execute arbitrary SQL commands and bypass Login via the email or password Login parameters.	9.8	More Details
CVE-2024-41476	AMTT Hotel Broadband Operation System (HiBOS) V3.0.3.151204 and before is vulnerable to SQL Injection via /manager/card/card_detail.php.	9.8	More Details
CVE-2024-41570	An Unauthenticated Server-Side Request Forgery (SSRF) in demon callback handling in Havoc 2 0.7 allows attackers to send arbitrary network traffic originating from the team server.	9.8	More Details
CVE-2024-41577	An arbitrary file upload vulnerability in the Ueditor component of productinfoquick v1.0 allows attackers to execute arbitrary code via uploading a crafted PNG file.	9.8	More Details
CVE-2024-7569	An information disclosure vulnerability in Ivanti ITSM on-prem and Neurons for ITSM versions 2023.4 and earlier allows an unauthenticated attacker to obtain the OIDC client secret via debug information.	9.6	More Details
CVE-2024-38108	Azure Stack Hub Spoofing Vulnerability	9.3	More Details
CVE-2024-42037	Vulnerability of uncaught exceptions in the Graphics module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	9.3	More Details
CVE-2024-38160	Windows Network Virtualization Remote Code Execution Vulnerability	9.1	More Details
CVE-2024-38159	Windows Network Virtualization Remote Code Execution Vulnerability	9.1	More Details
CVE-2024-38109	An authenticated attacker can exploit an Server-Side Request Forgery (SSRF) vulnerability in Microsoft Azure Health Bot to elevate privileges over a network.	9.1	More Details
CVE-2024-42167	The function "generate_app_certificates" in controllers/saml2/saml2.js of FIWARE Keyrock <= 8.4 does not neutralize special elements used in an OS Command properly. This allows an authenticated user with permissions to create applications to execute commands by creating an application with a malicious organisationname.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37287	A flaw allowing arbitrary code execution was discovered in Kibana. An attacker with access to ML and Alerting connector features, as well as write access to internal ML indices can trigger a prototype pollution vulnerability, ultimately leading to arbitrary code execution.	9.1	More Details
CVE-2024-43121	Improper Privilege Management vulnerability in realmag777 HUSKY allows Privilege Escalation.This issue affects HUSKY: from n/a through 1.3.6.1.	9.1	More Details
CVE-2024-42166	The function "generate_app_certificates" in lib/app_certificates.js of FIWARE Keyrock <= 8.4 does not neutralize special elements used in an OS Command properly. This allows an authenticated user with permissions to create applications to execute commands by creating an application with a malicious name.	9.1	More Details
CVE-2024-21876	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability via a URL parameter in Enphase IQ Gateway (formerly known as Envoy) allows an unautheticated attacker to access or create arbitratry files.This issue affects Envoy: from 4.x to 8.x and < 8.2.4225.	9.1	More Details
CVE-2024-36461	Within Zabbix, users have the ability to directly modify memory pointers in the JavaScript engine.	9.1	More Details
CVE-2024-37023	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters.	9.1	More Details
CVE-2024-39815	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service. A specially-crafted HTTP request to pre-authentication resources can crash the service.	9.1	More Details
CVE-2024-41940	A vulnerability has been identified in SINEC NMS (All versions < V3.0). The affected application does not properly validate user input to a privileged command queue. This could allow an authenticated attacker to execute OS commands with elevated privileges.	9.1	More Details
CVE-2024-42366	VRCX is an assistant/companion application for VRChat. In versions prior to 2024.03.23, a CefSharp browser with over-permission and cross-site scripting via overlay notification can be combined to result in remote command execution. These vulnerabilities are patched in VRCX 2023.12.24. In addition to the patch, VRCX maintainers worked with the VRC team and blocked the older version of VRCX on the VRC's API side. Users who use the older version of VRCX must update their installation to continue using VRCX.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-39091	An OS command injection vulnerability in the ccm_debug component of MIPC Camera firmware prior to v5.4.1.240424171021 allows attackers within the same network to execute arbitrary code via a crafted HTML request.	8.8	More Details
CVE-2024-38120	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-42743	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setSyslogCfg . Authenticated Attackers can send malicious packet to execute arbitrary commands.	8.8	More Details
CVE-2024-38128	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-42742	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setUrlFilterRules. Authenticated Attackers can send malicious packet to execute arbitrary commands.	8.8	More Details
CVE-2024-42741	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setL2tpServerCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38121	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-7265	Incorrect User Management vulnerability in Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy EZD RP allows logged-in user to change the password of any user, including root user, which could lead to privilege escalation. This issue affects EZD RP: from 15 before 15.84, from 16 before 16.15, from 17 before 17.2.	8.8	More Details
CVE-2023-48171	An issue in OWASP DefectDojo before v.1.5.3.1 allows a remote attacker to escalate privileges via the user permissions component.	8.8	More Details
CVE-2024-38154	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-5290	An issue was discovered in Ubuntu wpa_supplicant that resulted in loading of arbitrary shared objects, which allows a local unprivileged attacker to escalate privileges to the user that wpa_supplicant runs as (usually root). Membership in the netdev group or access to the dbus interface of wpa_supplicant allow an unprivileged user to specify an arbitrary path to a module to be loaded by the wpa_supplicant process; other escalation paths might exist.	8.8	More Details
CVE-2024-7584	A vulnerability, which was classified as critical, was found in Tenda i22 1.0.0.3(4687). Affected is the function formApPortalPhoneAuth of the file /goform/apPortalPhoneAuth. The manipulation of the argument data leads to 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-2024-42627	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/snippet/delete/3.	8.8	More Details
CVE-2024-42626	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/snippet/add.	8.8	More Details
CVE-2024-7585	A vulnerability has been found in Tenda i22 1.0.0.3(4687) and classified as critical. Affected by this vulnerability is the function formApPortalWebAuth of the file /goform/apPortalAuth. The manipulation of the argument webUserName/webUserPassword leads to 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-2024-42625	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/layout/add	8.8	More Details
CVE-2024-43044	Jenkins 2.470 and earlier, LTS 2.452.3 and earlier allows agent processes to read arbitrary files from the Jenkins controller file system by using the `ClassLoaderProxy#fetchJar` method in the Remoting library.	8.8	More Details
CVE-2024-42744	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setModifyVpnUser. Authenticated Attackers can send malicious packet to execute arbitrary commands.	8.8	More Details
CVE-2024-7583	A vulnerability, which was classified as critical, has been found in Tenda i22 1.0.0.3(4687). This issue affects the function formApPortalOneKeyAuth of the file /goform/apPortalOneKeyAuth. The manipulation of the argument data leads to 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-2024-42745	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setUPnPCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands.	8.8	More Details
CVE-2024-42747	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setWanIeCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42748	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setWiFiWpsCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands.	8.8	More Details
CVE-2024-7582	A vulnerability classified as critical was found in Tenda i22 1.0.0.3(4687). This vulnerability affects the function formApPortalAccessCodeAuth of the file /goform/apPortalAccessCodeAuth. The manipulation of the argument accessCode/data/acceInfo leads to 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-2024-7615	A vulnerability was found in Tenda FH1206 1.2.0.8. It has been declared as critical. Affected by this vulnerability is the function fromSafeClientFilter/fromSafeMacFilter/fromSafeUrlFilter. The manipulation 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-2024-7614	A vulnerability was found in Tenda FH1206 1.2.0.8(8155). It has been classified as critical. Affected is the function fromqossetting of the file /goform/qossetting. The manipulation of the argument page leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-7581	A vulnerability classified as critical has been found in Tenda A301 15.13.08.12. This affects the function formWifiBasicSet of the file /goform/WifiBasicSet. The manipulation of the argument security 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-2024-38130	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-7613	A vulnerability was found in Tenda FH1206 1.2.0.8(8155) and classified as critical. This issue affects the function fromGstDhcpSetSer of the file /goform/GstDhcpSetSer. The manipulation of the argument dips leads to 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-2024-38131	Clipboard Virtual Channel Extension Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-7557	A vulnerability was found in OpenShift AI that allows for authentication bypass and privilege escalation across models within the same namespace. When deploying AI models, the UI provides the option to protect models with authentication. However, credentials from one model can be used to access other models and APIs within the same namespace. The exposed ServiceAccount tokens, visible in the UI, can be utilized with oc --token={token} to exploit the elevated view privileges associated with the ServiceAccount, leading to unauthorized access to additional resources.	8.8	More Details
CVE-2024-7399	Improper limitation of a pathname to a restricted directory vulnerability in Samsung MagicINFO 9 Server version before 21.1050 allows attackers to write arbitrary file as system authority.	8.8	More Details
CVE-2024-7707	A vulnerability was found in Tenda FH1206 02.03.01.35 and classified as critical. Affected by this issue is the function formSafeEmailFilter of the file /goform/SafeEmailFilter of the component HTTP POST Request Handler. The manipulation of the argument page leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-38144	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	8.8	More Details
CVE-2024-42624	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/page/delete/10.	8.8	More Details
CVE-2024-36131	An insecure deserialization vulnerability in web component of EPMM prior to 12.1.0.1 allows an authenticated remote attacker to execute arbitrary commands on the underlying operating system of the appliance.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42623	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/layout/delete/1	8.8	More Details
CVE-2024-7150	The Slider by 10Web – Responsive Image Slider plugin for WordPress is vulnerable to time-based SQL Injection via the 'id' parameter in all versions up to, and including, 1.2.57 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-2024-7348	Time-of-check Time-of-use (TOCTOU) race condition in pg_dump in PostgreSQL allows an object creator to execute arbitrary SQL functions as the user running pg_dump, which is often a superuser. The attack involves replacing another relation type with a view or foreign table. The attack requires waiting for pg_dump to start, but winning the race condition is trivial if the attacker retains an open transaction. Versions before PostgreSQL 16.4, 15.8, 14.13, 13.16, and 12.20 are affected.	8.8	More Details
CVE-2024-42737	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in delBlacklist. Authenticated Attackers can send malicious packet to execute arbitrary commands.	8.8	More Details
CVE-2024-42738	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setDmzCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands.	8.8	More Details
CVE-2024-42739	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setAccessDeviceCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands.	8.8	More Details
CVE-2024-21879	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability through an url parameter of an authenticated enpoint in Enphase IQ Gateway (formerly known as Envoy) allows OS Command Injection.This issue affects Envoy: from 4.x to 8.x and < 8.2.4225.	8.8	More Details
CVE-2024-42038	Vulnerability of PIN enhancement failures in the screen lock module Impact: Successful exploitation of this vulnerability may affect service confidentiality, integrity, and availability.	8.8	More Details
CVE-2024-29831	Improper Input Validation vulnerability in Apache DolphinScheduler. An authenticated user can cause arbitrary, unsandboxed javascript to be executed on the server. If you are using the switch task plugin, please upgrade to version 3.2.2.	8.8	More Details
CVE-2024-41939	A vulnerability has been identified in SINEC NMS (All versions < V3.0). The affected application does not properly enforce authorization checks. This could allow an authenticated attacker to bypass the checks and elevate their privileges on the application.	8.8	More Details
CVE-2024-42628	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/snippet/edit/3.	8.8	More Details
CVE-2024-42629	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/page/edit/10.	8.8	More Details
CVE-2024-7548	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to time-based SQL Injection via the 'order' parameter in all versions up to, and including, 4.2.6.9.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for 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-2024-42630	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/plugin/file_manager/create_file.	8.8	More Details
CVE-2024-42631	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/layout/edit/1.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42632	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/page/add.	8.8	More Details
CVE-2024-36446	The provisioning manager component of Mitel MiVoice MX-ONE through 7.6 SP1 could allow an authenticated attacker to conduct an authentication bypass attack due to improper access control. A successful exploit could allow an attacker to bypass the authorization schema.	8.8	More Details
CVE-2024-38180	Windows SmartScreen Security Feature Bypass Vulnerability	8.8	More Details
CVE-2024-40475	SourceCodester Best House Rental Management System v1.0 is vulnerable to Incorrect Access Control via /rental/payment_report.php, /rental/balance_report.php, /rental/invoices.php, /rental/tenants.php, and /rental/users.php.	8.8	More Details
CVE-2024-7492	The MainWP Child Reports plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.2. This is due to missing or incorrect nonce validation on the network_options_action() function. This makes it possible for unauthenticated attackers to update arbitrary options that can be leveraged for privilege escalation via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. This is only exploitable on multisite instances.	8.8	More Details
CVE-2024-7561	The The Next theme for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.1.0 via deserialization of untrusted input from the wpeden_post_meta 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 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-2024-41475	Gnuboard g6 6.0.7 is vulnerable to Session hijacking due to a CORS misconfiguration.	8.8	More Details
CVE-2024-40488	A Cross-Site Request Forgery (CSRF) vulnerability was found in the Kashipara Live Membership System v1.0. This could lead to an attacker tricking the administrator into deleting valid member data via a crafted HTML page, as demonstrated by a Delete Member action at the /delete_members.php.	8.8	More Details
CVE-2024-7486	The MultiPurpose theme for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.2.0 via deserialization of untrusted input through the 'wpeden_post_meta' post meta. 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-2024-6823	The Media Library Assistant plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation involving the mla-inline-edit-upload-scripts AJAX action in all versions up to, and including, 3.18. This makes it possible for authenticated attackers, with Author-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2024-6891	Attackers with a valid username and password can exploit a python code injection vulnerability during the natural login flow.	8.8	More Details
CVE-2024-6890	Password reset tokens are generated using an insecure source of randomness. Attackers who know the username of the Journyx installation user can bruteforce the password reset and change the administrator password.	8.8	More Details
CVE-2024-38189	Microsoft Project Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-6707	Attacker controlled files can be uploaded to arbitrary locations on the web server's filesystem by abusing a path traversal vulnerability.	8.8	More Details
CVE-2024-38114	Windows IP Routing Management Snapin Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38115	Windows IP Routing Management Snapin Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-38116	Windows IP Routing Management Snapin Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-5651	A flaw was found in the Fence Agents Remediation operator. This vulnerability can allow a Remote Code Execution (RCE) primitive by supplying an arbitrary command to execute in the --ssh-path/--telnet-path arguments. A low-privilege user, for example, a user with developer access, can create a specially crafted FenceAgentsRemediation for a fence agent supporting --ssh-path/--telnet-path arguments to execute arbitrary commands on the operator's pod. This RCE leads to a privilege escalation, first as the service account running the operator, then to another service account with cluster-admin privileges.	8.8	More Details
CVE-2024-0108	NVIDIA Jetson Linux contains a vulnerability in NvGPU where error handling paths in GPU MMU mapping code fail to clean up a failed mapping attempt. A successful exploit of this vulnerability may lead to denial of service, code execution, and escalation of privileges.	8.7	More Details
CVE-2024-42001	An improper authentication vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session.	8.6	More Details
CVE-2024-29082	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints.	8.6	More Details
CVE-2024-39651	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in WPWeb WooCommerce PDF Vouchers allows File Manipulation.This issue affects WooCommerce PDF Vouchers: from n/a before 4.9.5.	8.6	More Details
CVE-2024-6788	A remote unauthenticated attacker can use the firmware update feature on the LAN interface of the device to reset the password for the predefined, low-privileged user “user-app” to the default password.	8.6	More Details
CVE-2024-40500	Cross Site Scripting vulnerability in Martin Kucej i-librarian v.5.11.0 and before allows a local attacker to execute arbitrary code via the search function in the import component.	8.6	More Details
CVE-2024-6522	The Modern Events Calendar plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 7.12.1 via the 'mec_fes_form' AJAX function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	8.5	More Details
CVE-2024-42035	Permission control vulnerability in the App Multiplier module Impact:Successful exploitation of this vulnerability may affect functionality and confidentiality.	8.4	More Details
CVE-2024-34620	Improper privilege management in SumeNNService prior to SMR Aug-2024 Release 1 allows local attackers to start privileged service.	8.4	More Details
CVE-2024-38218	Microsoft Edge (HTML-based) Memory Corruption Vulnerability	8.4	More Details
CVE-2024-42356	Shopware is an open commerce platform. Prior to versions 6.6.5.1 and 6.5.8.13, the `context` variable is injected into almost any Twig Template and allows to access to current language, currency information. The context object allows also to switch for a short time the scope of the Context as a helper with a callable function. The function can be called also from Twig and as the second parameter allows any callable, it's possible to call from Twig any statically callable PHP function/method. It's not possible as customer to provide any Twig code, the attacker would require access to Administration to exploit it using Mail templates or using App Scripts. Update to Shopware 6.6.5.1 or 6.5.8.13 to receive a patch. For older versions of 6.1, 6.2, 6.3 and 6.4 corresponding security measures are also available via a plugin.	8.3	More Details
CVE-2024-36518	Zohocorp ManageEngine ADAudit Plus versions below 8110 are vulnerable to authenticated SQL Injection in attack surface analyzer's dashboard.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42163	Insufficiently random values for generating password reset token in FIWARE Keyrock <= 8.4 allow attackers to take over the account of any user by predicting the token for the password reset link.	8.3	More Details
CVE-2024-5527	Zohocorp ManageEngine ADAudit Plus versions below 8110 are vulnerable to authenticated SQL Injection in file auditing configuration.	8.3	More Details
CVE-2024-7570	Improper certificate validation in Ivanti ITSM on-prem and Neurons for ITSM Versions 2023.4 and earlier allows a remote attacker in a MITM position to craft a token that would allow access to ITSM as any user.	8.3	More Details
CVE-2024-42355	Shopware, an open ecommerce platform, has a new Twig Tag `sw_silent_feature_call` which silences deprecation messages while triggered in this tag. Prior to versions 6.6.5.1 and 6.5.8.13, it accepts as parameter a string the feature flag name to silence, but this parameter is not escaped properly and allows execution of code. Update to Shopware 6.6.5.1 or 6.5.8.13 to receive a patch. For older versions of 6.2, 6.3, and 6.4, corresponding security measures are also available via a plugin.	8.3	More Details
CVE-2024-42370	Litestar is an Asynchronous Server Gateway Interface (ASGI) framework. In versions 2.10.0 and prior, Litestar's `docs-preview.yml` workflow is vulnerable to Environment Variable injection which may lead to secret exfiltration and repository manipulation. This issue grants a malicious actor the permission to write issues, read metadata, and write pull requests. In addition, the `DOCS_PREVIEW_DEPLOY_TOKEN` is exposed to the attacker. Commit 84d351e96aaa2a1338006d6e7221eded161f517b contains a fix for this issue.	8.3	More Details
CVE-2024-5487	Zohocorp ManageEngine ADAudit Plus versions below 8110 are vulnerable to authenticated SQL Injection in attack surface analyzer's export option.	8.3	More Details
CVE-2024-7143	A flaw was found in the Pulp package. When a role-based access control (RBAC) object in Pulp is set to assign permissions on its creation, it uses the `AutoAddObjPermsMixin` (typically the add_roles_for_object_creator method). This method finds the object creator by checking the current authenticated user. For objects that are created within a task, this current user is set by the first user with any permissions on the task object. This means the oldest user with model/domain-level task permissions will always be set as the current user of a task, even if they didn't dispatch the task. Therefore, all objects created in tasks will have their permissions assigned to this oldest user, and the creating user will receive nothing.	8.3	More Details
CVE-2024-36034	Zohocorp ManageEngine ADAudit Plus versions below 8003 are vulnerable to authenticated SQL Injection in aggregate reports' search option.	8.3	More Details
CVE-2024-36035	Zohocorp ManageEngine ADAudit Plus versions below 8003 are vulnerable to authenticated SQL Injection in user session recording.	8.3	More Details
CVE-2024-38211	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	8.2	More Details
CVE-2024-36877	Micro-Star International Z-series motherboards (Z590, Z490, and Z790) and B-series motherboards (B760, B560, B660, and B460) with firmware 7D25v14, 7D25v17 to 7D25v19, and 7D25v1A to 7D25v1H was discovered to contain a write-what-where condition in the in the SW handler for SMI 0xE3. Motherboard's with the following chipsets are affected: Intel 300, Intel 400, Intel 500, Intel 600, Intel 700, AMD 300, AMD 400, AMD 500, AMD 600 and AMD 700.	8.2	More Details
CVE-2024-42374	BEx Web Java Runtime Export Web Service does not sufficiently validate an XML document accepted from an untrusted source. An attacker can retrieve information from the SAP ADS system and exhaust the number of XMLForm service which makes the SAP ADS rendering (PDF creation) unavailable. This affects the confidentiality and availability of the application.	8.2	More Details
CVE-2024-40479	A SQL injection vulnerability in "/admin/quizquestion.php" in Kashipara Online Exam System v1.0 allows remote attackers to execute arbitrary SQL commands via the "eid" parameter.	8.1	More Details
CVE-2024-29995	Windows Kerberos Elevation of Privilege Vulnerability	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36460	The front-end audit log allows viewing of unprotected plaintext passwords, where the passwords are displayed in plain text.	8.1	More Details
CVE-2024-41651	An issue in Prestashop v.8.1.7 and before allows a remote attacker to execute arbitrary code via the module upgrade functionality. NOTE: this is disputed by multiple parties, who report that exploitation requires that an attacker be able to hijack network requests made by an admin user (who, by design, is allowed to change the code that is running on the server).	8.1	More Details
CVE-2024-30188	File read and write vulnerability in Apache DolphinScheduler , authenticated users can illegally access additional resource files. This issue affects Apache DolphinScheduler: from 3.1.0 before 3.2.2. Users are recommended to upgrade to version 3.2.2, which fixes the issue.	8.1	More Details
CVE-2024-7589	A signal handler in sshd(8) may call a logging function that is not async-signal-safe. The signal handler is invoked when a client does not authenticate within the LoginGraceTime seconds (120 by default). This signal handler executes in the context of the sshd(8)'s privileged code, which is not sandboxed and runs with full root privileges. This issue is another instance of the problem in CVE-2024-6387 addressed by FreeBSD-SA-24:04.openssh. The faulty code in this case is from the integration of blacklistd in OpenSSH in FreeBSD. As a result of calling functions that are not async-signal-safe in the privileged sshd(8) context, a race condition exists that a determined attacker may be able to exploit to allow an unauthenticated remote code execution as root.	8.1	More Details
CVE-2024-42480	Kamaji is the Hosted Control Plane Manager for Kubernetes. In versions 1.0.0 and earlier, Kamaji uses an "open at the top" range definition in RBAC for etcd roles leading to some TCPs API servers being able to read, write, and delete the data of other control planes. This vulnerability is fixed in edge-24.8.2.	8.1	More Details
CVE-2024-40476	A Cross-Site Request Forgery (CSRF) vulnerability was found in SourceCodester Best House Rental Management System v1.0. This could lead to an attacker tricking the administrator into adding/modifying/deleting valid tenant data via a crafted HTML page, as demonstrated by a Delete Tenant action at the /rental/ajax.php?action=delete_tenant.	8.0	More Details
CVE-2024-38196	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38215	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-41908	A vulnerability has been identified in NX (All versions < V2406.3000). The affected applications contains an out of bounds read vulnerability while parsing specially crafted PRT files. This could allow an attacker to crash the application or execute code in the context of the current process.	7.8	More Details
CVE-2024-42257	In the Linux kernel, the following vulnerability has been resolved: ext4: use memtostr_pad() for s_volume_name As with the other strings in struct ext4_super_block, s_volume_name is not NUL terminated. The other strings were marked in commit 072ebb3bffe6 ("ext4: add nonstring annotations to ext4.h"). Using strscpy() isn't the right replacement for strncpy(); it should use memtostr_pad() instead.	7.8	More Details
CVE-2024-34622	Out-of-bounds write in appending paragraph in Samsung Notes prior to version 4.4.21.62 allows local attackers to potentially execute arbitrary code with Samsung Notes privilege.	7.8	More Details
CVE-2024-27442	An issue was discovered in Zimbra Collaboration (ZCS) 9.0 and 10.0. The zmmailboxdmgr binary, a component of ZCS, is intended to be executed by the zimbra user with root privileges for specific mailbox operations. However, an attacker can escalate privileges from the zimbra user to root, because of improper handling of input arguments. An attacker can execute arbitrary commands with elevated privileges, leading to local privilege escalation.	7.8	More Details
CVE-2024-42736	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in addBlacklist. Authenticated Attackers can send malicious packet to execute arbitrary commands.	7.8	More Details
CVE-2024-38152	Windows OLE Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-38084	Microsoft OfficePlus Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34623	Out-of-bounds write in applying connected information in Samsung Notes prior to version 4.4.21.62 allows local attackers to potentially execute arbitrary code with Samsung Notes privilege.	7.8	More Details
CVE-2023-50809	In certain Sonos products before S1 Release 11.12 and S2 release 15.9, the mt_7615.ko wireless driver does not properly validate an information element during negotiation of a WPA2 four-way handshake. This lack of validation leads to a stack buffer overflow. This can result in remote code execution within the kernel. This affects Amp, Arc, Arc SL, Beam, Beam Gen 2, Beam SL, and Five.	7.8	More Details
CVE-2024-38153	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38134	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-36398	A vulnerability has been identified in SINEC NMS (All versions < V3.0). The affected application executes a subset of its services as `NT AUTHORITY\SYSTEM`. This could allow a local attacker to execute operating system commands with elevated privileges.	7.8	More Details
CVE-2024-38125	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38150	Windows DWM Core Library Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38147	Microsoft DWM Core Library Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-41309	An issue in the Hardware info module of IT Solutions Enjay CRM OS v1.0 allows attackers to escape the restricted terminal environment and gain root-level privileges on the underlying system.	7.8	More Details
CVE-2024-41308	An issue in the Ping feature of IT Solutions Enjay CRM OS v1.0 allows attackers to escape the restricted terminal environment and gain root-level privileges on the underlying system.	7.8	More Details
CVE-2024-38142	Windows Secure Kernel Mode Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38141	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38135	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38195	Azure CycleCloud Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-38133	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38162	Azure Connected Machine Agent Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-7066	The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PDF files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-43199	Nagios NDOUtils before 2.1.4 allows privilege escalation from nagios to root because certain executable files are owned by the nagios user.	7.8	More Details
CVE-2024-38169	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-38127	Windows Hyper-V Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-0107	NVIDIA GPU Display Driver for Windows contains a vulnerability in the user mode layer, where an unprivileged regular user can cause an out-of-bounds read. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2024-38107	Windows Power Dependency Coordinator Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38098	Azure Connected Machine Agent Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38171	Microsoft PowerPoint Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-38191	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38117	NTFS Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38172	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-38177	Windows App Installer Spoofing Vulnerability	7.8	More Details
CVE-2024-38184	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38185	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38193	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38186	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38187	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40487	A Stored Cross Site Scripting (XSS) vulnerability was found in "/view_type.php" of Kashipara Live Membership System v1.0, which allows remote attackers to execute arbitrary code via membershipType parameter.	7.6	More Details
CVE-2024-41161	Use of hard-coded credentials vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication using hard-coded administrator credentials. These accounts cannot be disabled.	7.5	More Details
CVE-2024-6760	A logic bug in the code which disables kernel tracing for setuid programs meant that tracing was not disabled when it should have, allowing unprivileged users to trace and inspect the behavior of setuid programs. The bug may be used by an unprivileged user to read the contents of files to which they would not otherwise have access, such as the local password database.	7.5	More Details
CVE-2024-43131	Incorrect Authorization vulnerability in WPWeb Docket (WooCommerce Collections / Wishlist / Watchlist) allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Docket (WooCommerce Collections / Wishlist / Watchlist): from n/a before 1.7.0.	7.5	More Details
CVE-2024-40697	IBM Common Licensing 9.0 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 297895.	7.5	More Details
CVE-2024-35124	A vulnerability in the combination of the OpenBMC's FW1050.00 through FW1050.10, FW1030.00 through FW1030.50, and FW1020.00 through FW1020.60 default password and session management allow an attacker to gain administrative access to the BMC. IBM X-Force ID: 290674.	7.5	More Details
CVE-2024-33535	An issue was discovered in Zimbra Collaboration (ZCS) 9.0 and 10.0. The vulnerability involves unauthenticated local file inclusion (LFI) in a web application, specifically impacting the handling of the packages parameter. Attackers can exploit this flaw to include arbitrary local files without authentication, potentially leading to unauthorized access to sensitive information. The vulnerability is limited to files within a specific directory.	7.5	More Details
CVE-2023-31315	Improper validation in a model specific register (MSR) could allow a malicious program with ring0 access to modify SMM configuration while SMI lock is enabled, potentially leading to arbitrary code execution.	7.5	More Details
CVE-2024-41936	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication.	7.5	More Details
CVE-2024-43135	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Themewinter WPCafe allows PHP Local File Inclusion.This issue affects WPCafe: from n/a through 2.2.28.	7.5	More Details
CVE-2024-39338	axios 1.7.2 allows SSRF via unexpected behavior where requests for path relative URLs get processed as protocol relative URLs.	7.5	More Details
CVE-2024-38787	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Codection Import and export users and customers allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Import and export users and customers: from n/a through 1.26.8.	7.5	More Details
CVE-2024-42481	Skyport Daemon (skyportd) is the daemon for the Skyport Panel. By making thousands of folders & files (easy due to skyport's lack of rate limiting on createFolder. createFile), skyportd in a lot of cases will cause 100% CPU usage and an OOM, probably crashing the system. This is fixed in 0.2.2.	7.5	More Details
CVE-2024-7006	A null pointer dereference flaw was found in Libtiff via `tif_dirinfo.c`. This issue may allow an attacker to trigger memory allocation failures through certain means, such as restricting the heap space size or injecting faults, causing a segmentation fault. This can cause an application crash, eventually leading to a denial of service.	7.5	More Details
CVE-2024-37826	A NULL pointer dereference in vercot Serva v4.6.0 allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	7.5	More Details
CVE-2024-42485	Filament Excel enables excel export for Filament admin resources. The export download route `/filament-excel/{path}` allowed downloading any file without login when the webserver allows `../` in the URL. Patched with Version v2.3.3.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38747	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in HitPay Payment Solutions Pte Ltd HitPay Payment Gateway for WooCommerce allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects HitPay Payment Gateway for WooCommerce: from n/a through 4.1.3.	7.5	More Details
CVE-2024-42473	OpenFGA is an authorization/permission engine. OpenFGA v1.5.7 and v1.5.8 are vulnerable to authorization bypass when calling Check API with a model that uses `but not` and `from` expressions and a userset. Users should downgrade to v1.5.6 as soon as possible. This downgrade is backward compatible. As of time of publication, a patch is not available but OpenFGA's maintainers are planning a patch for inclusion in a future release.	7.5	More Details
CVE-2024-38699	Missing Authorization vulnerability in WP Swings Wallet System for WooCommerce allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Wallet System for WooCommerce: from n/a through 2.5.13.	7.5	More Details
CVE-2024-7697	Logical vulnerability in the mobile application (com.transsion.carlcare) may lead to user information leakage risks.	7.5	More Details
CVE-2024-37935	Missing Authorization vulnerability in anhvnit Woocommerce OpenPos allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Woocommerce OpenPos: from n/a through 6.4.4.	7.5	More Details
CVE-2024-41904	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V2.0). The affected application do not properly enforce restriction of excessive authentication attempts. This could allow an unauthenticated attacker to conduct brute force attacks against legitimate user credentials or keys.	7.5	More Details
CVE-2024-7693	Raiden MAILD Remote Management System from Team Johnlong Software has a Relative Path Traversal vulnerability, allowing unauthenticated remote attackers to read arbitrary file on the remote server.	7.5	More Details
CVE-2024-36462	Uncontrolled resource consumption refers to a software vulnerability where a attacker or system uses excessive resources, such as CPU, memory, or network bandwidth, without proper limitations or controls. This can cause a denial-of-service (DoS) attack or degrade the performance of the affected system.	7.5	More Details
CVE-2024-0113	NVIDIA Mellanox OS, ONYX, Skyway, and MetroX-3 XCC contain a vulnerability in the web support, where an attacker can cause a CGI path traversal by a specially crafted URI. A successful exploit of this vulnerability might lead to escalation of privileges and information disclosure.	7.5	More Details
CVE-2024-0101	NVIDIA Mellanox OS, ONYX, Skyway, MetroX-2 and MetroX-3 XC contain a vulnerability in ipfilter, where improper ipfilter definitions could enable an attacker to cause a failure by attacking the switch. A successful exploit of this vulnerability might lead to denial of service.	7.5	More Details
CVE-2024-43140	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in G5Theme Ultimate Bootstrap Elements for Elementor allows PHP Local File Inclusion.This issue affects Ultimate Bootstrap Elements for Elementor: from n/a through 1.4.4.	7.5	More Details
CVE-2022-23815	Improper bounds checking in APCB firmware may allow an attacker to perform an out of bounds write, corrupting the APCB entry, potentially leading to arbitrary code execution.	7.5	More Details
CVE-2024-42031	Access permission verification vulnerability in the Settings module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2024-37968	Windows DNS Spoofing Vulnerability	7.5	More Details
CVE-2024-6893	The "soap_cgi.pyc" API handler allows the XML body of SOAP requests to contain references to external entities. This allows an unauthenticated attacker to read local files, perform server-side request forgery, and overwhelm the web server resources.	7.5	More Details
CVE-2024-38126	Windows Network Address Translation (NAT) Denial of Service Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20451	Multiple vulnerabilities in the web-based management interface of Cisco Small Business SPA300 Series IP Phones and Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly. These vulnerabilities exist because HTTP packets are not properly checked for errors. An attacker could exploit this vulnerability by sending a crafted HTTP packet to the remote interface of an affected device. A successful exploit could allow the attacker to cause a DoS condition on the device.	7.5	More Details
CVE-2024-38132	Windows Network Address Translation (NAT) Denial of Service Vulnerability	7.5	More Details
CVE-2024-38138	Windows Deployment Services Remote Code Execution Vulnerability	7.5	More Details
CVE-2024-38145	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability	7.5	More Details
CVE-2024-38148	Windows Secure Channel Denial of Service Vulnerability	7.5	More Details
CVE-2024-41991	An issue was discovered in Django 5.0 before 5.0.8 and 4.2 before 4.2.15. The urlize and urlizetrunc template filters, and the AdminURLFieldWidget widget, are subject to a potential denial-of-service attack via certain inputs with a very large number of Unicode characters.	7.5	More Details
CVE-2024-41990	An issue was discovered in Django 5.0 before 5.0.8 and 4.2 before 4.2.15. The urlize() and urlizetrunc() template filters are subject to a potential denial-of-service attack via very large inputs with a specific sequence of characters.	7.5	More Details
CVE-2024-41989	An issue was discovered in Django 5.0 before 5.0.8 and 4.2 before 4.2.15. The floatformat template filter is subject to significant memory consumption when given a string representation of a number in scientific notation with a large exponent.	7.5	More Details
CVE-2024-38168	.NET and Visual Studio Denial of Service Vulnerability	7.5	More Details
CVE-2024-38178	Scripting Engine Memory Corruption Vulnerability	7.5	More Details
CVE-2024-36132	Insufficient verification of authentication controls in EPMM prior to 12.1.0.1 allows a remote attacker to bypass authentication and access sensitive resources.	7.5	More Details
CVE-2024-38198	Windows Print Spooler Elevation of Privilege Vulnerability	7.5	More Details
CVE-2024-34619	Improper input validation in librtp.so prior to SMR Aug-2024 Release 1 allows remote attackers to execute arbitrary code with system privilege. User interaction is required for triggering this vulnerability.	7.5	More Details
CVE-2023-20578	A TOCTOU (Time-Of-Check-Time-Of-Use) in SMM may allow an attacker with ring0 privileges and access to the BIOS menu or UEFI shell to modify the communications buffer potentially resulting in arbitrary code execution.	7.5	More Details
CVE-2024-38146	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability	7.5	More Details
CVE-2024-3913	An unauthenticated remote attacker can use this vulnerability to change the device configuration due to a file writeable for short time after system startup.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33003	Some OCC API endpoints in SAP Commerce Cloud allows Personally Identifiable Information (PII) data, such as passwords, email addresses, mobile numbers, coupon codes, and voucher codes, to be included in the request URL as query or path parameters. On successful exploitation, this could lead to a High impact on confidentiality and integrity of the application.	7.4	More Details
CVE-2024-42365	Asterisk is an open source private branch exchange (PBX) and telephony toolkit. Prior to asterisk versions 18.24.2, 20.9.2, and 21.4.2 and certified-asterisk versions 18.9-cert11 and 20.7-cert2, an AMI user with `write=originate` may change all configuration files in the `/etc/asterisk/` directory. This occurs because they are able to curl remote files and write them to disk, but are also able to append to existing files using the `FILE` function inside the `SET` application. This issue may result in privilege escalation, remote code execution and/or blind server-side request forgery with arbitrary protocol. Asterisk versions 18.24.2, 20.9.2, and 21.4.2 and certified-asterisk versions 18.9-cert11 and 20.7-cert2 contain a fix for this issue.	7.4	More Details
CVE-2024-37015	An issue was discovered in Ada Web Server 20.0. When configured to use SSL (which is not the default setting), the SSL/TLS used to establish connections to external services is done without proper hostname validation. This is exploitable by man-in-the-middle attackers.	7.4	More Details
CVE-2024-7637	A vulnerability was found in code-projects Online Polling 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file registeracc.php of the component Registration. The manipulation of the argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-7636	A vulnerability was found in code-projects Simple Ticket Booking 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file authenticate.php of the component Login. The manipulation of the argument email/password leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2023-31348	A DLL hijacking vulnerability in AMD µProf could allow an attacker to achieve privilege escalation, potentially resulting in arbitrary code execution.	7.3	More Details
CVE-2024-34614	Out-of-bound write in libsmat.so prior to SMR Aug-2024 Release 1 allows local attackers to execute arbitrary code.	7.3	More Details
CVE-2024-34612	Out-of-bound write in libcodec2secmp4vdec.so prior to SMR Aug-2024 Release 1 allows local attackers to execute arbitrary code.	7.3	More Details
CVE-2024-7682	A vulnerability was found in code-projects Job Portal 1.0. It has been rated as critical. This issue affects some unknown processing of the file rw_i_nat.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2023-31349	Incorrect default permissions in the AMD µProf installation directory could allow an attacker to achieve privilege escalation, potentially resulting in arbitrary code execution.	7.3	More Details
CVE-2024-7553	Incorrect validation of files loaded from a local untrusted directory may allow local privilege escalation if the underlying operating systems is Windows. This may result in the application executing arbitrary behaviour determined by the contents of untrusted files. This issue affects MongoDB Server v5.0 versions prior to 5.0.27, MongoDB Server v6.0 versions prior to 6.0.16, MongoDB Server v7.0 versions prior to 7.0.12, MongoDB Server v7.3 versions prior 7.3.3, MongoDB C Driver versions prior to 1.26.2 and MongoDB PHP Driver versions prior to 1.18.1. Required Configuration: Only environments with Windows as the underlying operating system is affected by this issue	7.3	More Details
CVE-2024-7681	A vulnerability was found in code-projects College Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file login.php of the component Login Page. The manipulation of the argument email/password leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38202	Summary Microsoft was notified that an elevation of privilege vulnerability exists in Windows Update, potentially enabling an attacker with basic user privileges to reintroduce previously mitigated vulnerabilities or circumvent some features of Virtualization Based Security (VBS). However, an attacker attempting to exploit this vulnerability requires additional interaction by a privileged user to be successful. Microsoft has developed a security update to mitigate this threat which was made available October 08, 2024 and is provided in the Security Updates table of this CVE for customers to download. Note: Depending on your version of Windows, additional steps may be required to update Windows Recovery Environment (WinRE) to be protected from this vulnerability. Please refer to the FAQ section for more information. Guidance for customers who cannot immediately implement the update is provided in the Recommended Actions section of this CVE to help reduce the risks associated with this vulnerability and to protect their systems. If there are any further updates regarding mitigations for this vulnerability, this CVE will be updated and customers will be notified. We highly encourage customers to subscribe to Security Update Guide notifications to receive an alert if an update occurs. Details A security researcher informed Microsoft of an elevation of privilege vulnerability in Windows Update potentially enabling an attacker with basic user privileges to reintroduce previously mitigated vulnerabilities or circumvent some features of VBS. For exploitation to succeed, an attacker must trick or convince an Administrator or a user with delegated permissions into performing a system restore which inadvertently triggers the vulnerability. Microsoft has developed a security update to mitigate this threat which was made available October 08, 2024 and is provided in the Security Updates table of this CVE for customers to download. Note: Depending on your version of Windows, additional steps may be required to update Windows Recovery Environment (WinRE) to be protected from this vulnerability. Please refer to the FAQ section for more information. Guidance for customers who cannot immediately implement the update is provided in the Recommended Actions section of this CVE to help reduce the risks associated with this vulnerability and to protect their systems. If there are any further... See more at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38202	7.3	More Details
CVE-2024-42357	Shopware is an open commerce platform. Prior to versions 6.6.5.1 and 6.5.8.13, the Shopware application API contains a search functionality which enables users to search through information stored within their Shopware instance. The searches performed by this function can be aggregated using the parameters in the `aggregations` object. The `name` field in this `aggregations` object is vulnerable SQL-injection and can be exploited using SQL parameters. Update to Shopware 6.6.5.1 or 6.5.8.13 to receive a patch. For older versions of 6.1, 6.2, 6.3, and 6.4, corresponding security measures are also available via a plugin.	7.3	More Details
CVE-2024-42005	An issue was discovered in Django 5.0 before 5.0.8 and 4.2 before 4.2.15. QuerySet.values() and values_list() methods on models with a JSONField are subject to SQL injection in column aliases via a crafted JSON object key as a passed *arg.	7.3	More Details
CVE-2024-7578	A vulnerability was found in Alien Technology ALR-F800 up to 19.10.24.00. It has been classified as critical. Affected is an unknown function of the file /var/www/cmd.php. The manipulation of the argument cmd leads to improper authorization. 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.	7.3	More Details
CVE-2024-7635	A vulnerability was found in code-projects Simple Ticket Booking 1.0. It has been classified as critical. Affected is an unknown function of the file register_insert.php of the component Registration Handler. The manipulation of the argument name/email/dob/password/Gender/phone 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-2024-7740	A vulnerability has been found in wanglongcn ltcms 1.0.20 and classified as critical. This vulnerability affects the function download of the file /api/test/download of the component API Endpoint. The manipulation of the argument url leads to server-side request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2024-7742	A vulnerability was found in wanglongcn ltcms 1.0.20. It has been classified as critical. Affected is the function multiDownload of the file /api/file/multiDownload of the component API Endpoint. The manipulation of the argument file leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2024-7743	A vulnerability was found in wanglongcn ltcms 1.0.20. It has been declared as critical. Affected by this vulnerability is the function downloadUrl of the file /api/file/downloadUrl of the component API Endpoint. The manipulation of the argument file leads to server-side request forgery. 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.	7.3	More Details
CVE-2023-31341	Insufficient validation of the Input Output Control (IOCTL) input buffer in AMD ?Prof may allow an authenticated attacker to cause an out-of-bounds write, potentially causing a Windows® OS crash, resulting in denial of service.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37382	An issue discovered in import host feature in Ab Initio Metadata Hub and Authorization Gateway before 4.3.1.1 allows attackers to run arbitrary code via crafted modification of server configuration.	7.2	More Details
CVE-2024-42062	CloudStack account-users by default use username and password based authentication for API and UI access. Account-users can generate and register randomised API and secret keys and use them for the purpose of API-based automation and integrations. Due to an access permission validation issue that affects Apache CloudStack versions 4.10.0 up to 4.19.1.0, domain admin accounts were found to be able to query all registered account-users API and secret keys in an environment, including that of a root admin. An attacker who has domain admin access can exploit this to gain root admin and other-account privileges and perform malicious operations that can result in compromise of resources integrity and confidentiality, data loss, denial of service and availability of CloudStack managed infrastructure. Users are recommended to upgrade to Apache CloudStack 4.18.2.3 or 4.19.1.1, or later, which addresses this issue. Additionally, all account-user API and secret keys should be regenerated.	7.2	More Details
CVE-2024-3659	Firmware in KAON AR2140 routers prior to version 4.2.16 is vulnerable to a shell command injection via sending a crafted request to one of the endpoints. In order to exploit this vulnerability, one has to have access to the administrative portal of the router.	7.2	More Details
CVE-2024-41976	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.1), RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2) (All versions < V8.1), SCALANCE M804PB (6GK5804-0AP00-2AA2) (All versions < V8.1), SCALANCE M812-1 ADSL-Router family (All versions < V8.1), SCALANCE M816-1 ADSL-Router family (All versions < V8.1), SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) (All versions < V8.1), SCALANCE M874-2 (6GK5874-2AA00-2AA2) (All versions < V8.1), SCALANCE M874-3 (6GK5874-3AA00-2AA2) (All versions < V8.1), SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2) (All versions < V8.1), SCALANCE M876-3 (6GK5876-3AA02-2BA2) (All versions < V8.1), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.1), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.1), SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) (All versions < V8.1), SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) (All versions < V8.1), SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1) (All versions < V8.1), SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1) (All versions < V8.1), SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) (All versions < V8.1), SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1) (All versions < V8.1), SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1) (All versions < V8.1), SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1) (All versions < V8.1), SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) (All versions < V8.1), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.1), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All versions < V8.1), SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2) (All versions < V8.1). Affected devices do not properly validate input in specific VPN configuration fields. This could allow an authenticated remote attacker to execute arbitrary code on the device.	7.2	More Details
CVE-2021-26344	An out of bounds memory write when processing the AMD PSP1 Configuration Block (APCB) could allow an attacker with access the ability to modify the BIOS image, and the ability to sign the resulting image, to potentially modify the APCB block resulting in arbitrary code execution.	7.2	More Details
CVE-2024-7560	The News Flash theme for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.1.0 via deserialization of untrusted input from the newsflash_post_meta meta value. This makes it possible for authenticated attackers, with Editor-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.	7.2	More Details
CVE-2024-7694	ThreatSonar Anti-Ransomware from TeamT5 does not properly validate the content of uploaded files. Remote attackers with administrator privileges on the product platform can upload malicious files, which can be used to execute arbitrary system command on the server.	7.2	More Details
CVE-2024-21880	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability via the url parameter of an authenticated enpoint in Enphase IQ Gateway (formerly known as Enphase) allows OS Command Injection.This issue affects Envoy: 4.x <= 7.x	7.2	More Details
CVE-2024-41942	JupyterHub is software that allows one to create a multi-user server for Jupyter notebooks. Prior to versions 4.1.6 and 5.1.0, if a user is granted the `admin:users` scope, they may escalate their own privileges by making themselves a full admin user. The impact is relatively small in that `admin:users` is already an extremely privileged scope only granted to trusted users. In effect, `admin:users` is equivalent to `admin=True`, which is not intended. Note that the change here only prevents escalation to the built-in JupyterHub admin role that has unrestricted permissions. It does not prevent users with e.g. `groups` permissions from granting themselves or other users permissions via group membership, which is intentional. Versions 4.1.6 and 5.1.0 fix this issue.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43213	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in MultiVendorX WC Marketplace allows Reflected XSS.This issue affects WC Marketplace: from n/a through 4.1.17.	7.1	More Details
CVE-2024-43156	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in AddonMaster Post Grid Master allows Reflected XSS.This issue affects Post Grid Master: from n/a through 3.4.10.	7.1	More Details
CVE-2024-40892	A weak credential vulnerability exists in Firewalla Box Software versions before 1.979. This vulnerability allows a physically close attacker to use the license UUID for authentication and provision SSH credentials over the Bluetooth Low-Energy (BTLE) interface. Once an attacker gains access to the LAN, they could log into the SSH interface using the provisioned credentials. The license UUID can be acquired through plain-text Bluetooth sniffing, reading the QR code on the bottom of the device, or brute-forcing the UUID (though this is less likely).	7.1	More Details
CVE-2024-38502	An unauthenticated remote attacker may use stored XSS vulnerability to obtain information from a user or reboot the affected device once.	7.1	More Details
CVE-2023-41884	ZoneMinder is a free, open source Closed-circuit television software application. In WWW/AJAX/watch.php, Line: 51 takes a few parameter in sql query without sanitizing it which makes it vulnerable to sql injection. This vulnerability is fixed in 1.36.34.	7.1	More Details
CVE-2024-43127	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPFactory Products, Order & Customers Export for WooCommerce allows Reflected XSS.This issue affects Products, Order & Customers Export for WooCommerce: from n/a through 2.0.11.	7.1	More Details
CVE-2024-43126	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Sender Sender – Newsletter, SMS and Email Marketing Automation for WooCommerce allows Reflected XSS.This issue affects Sender – Newsletter, SMS and Email Marketing Automation for WooCommerce: from n/a through 2.6.14.	7.1	More Details
CVE-2024-43217	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Pierre Lebedel Kodex Posts likes allows Reflected XSS.This issue affects Kodex Posts likes: from n/a through 2.5.0.	7.1	More Details
CVE-2024-38170	Microsoft Excel Remote Code Execution Vulnerability	7.1	More Details
CVE-2024-43233	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BannerSky BSK Forms Blacklist allows Reflected XSS.This issue affects BSK Forms Blacklist: from n/a through 3.8.	7.1	More Details
CVE-2024-43163	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Parcel Panel ParcelPanel allows Reflected XSS.This issue affects ParcelPanel: from n/a through 4.3.2.	7.1	More Details
CVE-2024-43220	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in 10Web Form Builder Team Form Maker by 10Web allows Reflected XSS.This issue affects Form Maker by 10Web: from n/a through 1.15.26.	7.1	More Details
CVE-2024-38724	Cross-Site Request Forgery (CSRF), Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Muhammad Rehman Contact Form 7 Summary and Print allows Stored XSS.This issue affects Contact Form 7 Summary and Print: from n/a through 1.2.5.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41977	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.1), RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2) (All versions < V8.1), SCALANCE M804PB (6GK5804-0AP00-2AA2) (All versions < V8.1), SCALANCE M812-1 ADSL-Router family (All versions < V8.1), SCALANCE M816-1 ADSL-Router family (All versions < V8.1), SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) (All versions < V8.1), SCALANCE M874-2 (6GK5874-2AA00-2AA2) (All versions < V8.1), SCALANCE M874-3 (6GK5874-3AA00-2AA2) (All versions < V8.1), SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2) (All versions < V8.1), SCALANCE M876-3 (6GK5876-3AA02-2BA2) (All versions < V8.1), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.1), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.1), SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) (All versions < V8.1), SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) (All versions < V8.1), SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1) (All versions < V8.1), SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1) (All versions < V8.1), SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) (All versions < V8.1), SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1) (All versions < V8.1), SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1) (All versions < V8.1), SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1) (All versions < V8.1), SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) (All versions < V8.1), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.1), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All versions < V8.1), SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2) (All versions < V8.1). Affected devices do not properly enforce isolation between user sessions in their web server component. This could allow an authenticated remote attacker to escalate their privileges on the devices.	7.1	More Details
CVE-2024-5849	An unauthenticated remote attacker may use a reflected XSS vulnerability to obtain information from a user or reboot the affected device once.	7.1	More Details
CVE-2024-22069	There is a permission and access control vulnerability of ZTE's ZXV10 XT802/ET301 product.Attackers with common permissions can log in the terminal web and change the password of the administrator illegally by intercepting requests to change the passwords.	7.1	More Details
CVE-2024-38106	Windows Kernel Elevation of Privilege Vulnerability	7.0	More Details
CVE-2024-38136	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability	7.0	More Details
CVE-2024-38137	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-23817	Insufficient checking of memory buffer in ASP Secure OS may allow an attacker with a malicious TA to read/write to the ASP Secure OS kernel virtual address space, potentially leading to privilege escalation.	7.0	More Details
CVE-2024-38201	Azure Stack Hub Elevation of Privilege Vulnerability	7.0	More Details
CVE-2024-38157	Azure IoT SDK Remote Code Execution Vulnerability	7.0	More Details
CVE-2024-38158	Azure IoT SDK Remote Code Execution Vulnerability	7.0	More Details
CVE-2024-42033	Access control vulnerability in the security verification module mpact: Successful exploitation of this vulnerability will affect integrity and confidentiality.	6.9	More Details
CVE-2024-41711	A vulnerability in the Mitel 6800 Series, 6900 Series, and 6900w Series SIP Phones, including the 6970 Conference Unit, through R6.4.0.HF1 (R6.4.0.136) could allow an unauthenticated attacker with physical access to the phone to conduct an argument injection attack, due to insufficient parameter sanitization. A successful exploit could allow an attacker to execute arbitrary commands within the context of the system.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42740	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setLedCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands.	6.8	More Details
CVE-2023-40261	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR17, 4.0.0 SR07, 4.1.0 SR04, 4.2.0 SR04, and 4.3.0 SR02 fails to validate file attributes during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk.	6.8	More Details
CVE-2023-24064	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR4 fails to validate /etc/initab during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk.	6.8	More Details
CVE-2023-33206	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR16, 4.0.0 SR06, 4.1.0 SR04, 4.2.0 SR03, and 4.3.0 SR01 fails to validate symlinks during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk.	6.8	More Details
CVE-2023-24063	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR10 fails to validate /etc/mtab during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk.	6.8	More Details
CVE-2024-3035	A permission check vulnerability in GitLab CE/EE affecting all versions starting from 8.12 prior to 17.0.6, 17.1 prior to 17.1.4, and 17.2 prior to 17.2.2 allowed for LFS tokens to read and write to the user owned repositories.	6.8	More Details
CVE-2024-38161	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	6.8	More Details
CVE-2023-26211	An improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiSOAR 7.3.0 through 7.3.2 allows an authenticated, remote attacker to inject arbitrary web script or HTML via the Communications module.	6.8	More Details
CVE-2023-24062	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR12, 4.0.0 SR04, 4.1.0 SR02, and 4.2.0 SR01 fails to validate the directory structure of the root file system during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk.	6.8	More Details
CVE-2024-41710	A vulnerability in the Mitel 6800 Series, 6900 Series, and 6900w Series SIP Phones, including the 6970 Conference Unit, through R6.4.0.HF1 (R6.4.0.136) could allow an authenticated attacker with administrative privilege to conduct an argument injection attack, due to insufficient parameter sanitization during the boot process. A successful exploit could allow an attacker to execute arbitrary commands within the context of the system.	6.8	More Details
CVE-2024-40893	Multiple authenticated operating system (OS) command injection vulnerabilities exist in Firewalla Box Software versions before 1.979. A physically close attacker that is authenticated to the Bluetooth Low-Energy (BTLE) interface can use the network configuration service to inject commands in various configuration parameters including networkConfig.Interface.Phy.Eth0.Extra.PingTestIP, networkConfig.Interface.Phy.Eth0.Extra.DNSTestDomain, and networkConfig.Interface.Phy.Eth0.Gateway6. Additionally, because the configuration can be synced to the Firewalla cloud, the attacker may be able to persist access even after hardware resets and firmware re-flashes.	6.8	More Details
CVE-2024-38223	Windows Initial Machine Configuration Elevation of Privilege Vulnerability	6.8	More Details
CVE-2024-41905	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V2.0). The affected application do not have access control for accessing the files. This could allow an authenticated attacker with low privilege's to get access to sensitive information.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21302	Summary: Microsoft was notified that an elevation of privilege vulnerability exists in Windows based systems supporting Virtualization Based Security (VBS), including a subset of Azure Virtual Machine SKUS. This vulnerability enables an attacker with administrator privileges to replace current versions of Windows system files with outdated versions. By exploiting this vulnerability, an attacker could reintroduce previously mitigated vulnerabilities, circumvent some features of VBS, and exfiltrate data protected by VBS. Microsoft is developing a security update to mitigate this threat, but it is not yet available. Guidance to help customers reduce the risks associated with this vulnerability and to protect their systems until the mitigation is available in a Windows security update is provided in the Recommended Actions section of this CVE. This CVE will be updated when the mitigation is available in a Windows security update. We highly encourage customers to subscribe to Security Update Guide notifications to receive an alert when this update occurs. Update: August 13, 2024 Microsoft has released the August 2024 security updates that include an opt-in revocation policy mitigation to address this vulnerability. Customers running affected versions of Windows are encouraged to review KB5042562: Guidance for blocking rollback of virtualization-based security related updates to assess if this opt-in policy meets the needs of their environment before implementing this mitigation. There are risks associated with this mitigation that should be understood prior to applying it to your systems. Detailed information about these risks is also available in KB5042562. Details: A security researcher informed Microsoft of an elevation of privilege vulnerability in Windows 10, Windows 11, Windows Server 2016, and higher based systems including Azure Virtual Machines (VM) that support VBS. For more information on Windows versions and VM SKUs supporting VBS, reference: Virtualization-based Security (VBS)	Microsoft Learn. The vulnerability enables an attacker with administrator privileges on the target system to replace current Windows system files with outdated versions. Successful exploitation provides an attacker with the ability to reintroduce previously mitigated vulnerabilities, circumvent VBS security features, and exfiltrate data protected by VBS. Microsoft is developing a security... See more at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21302	6.7	More Details
CVE-2024-41681	A vulnerability has been identified in Location Intelligence family (All versions < V4.4). The web server of affected products is configured to support weak ciphers by default. This could allow an unauthenticated attacker in an on-path position to to read and modify any data passed over the connection between legitimate clients and the affected device.	6.7	More Details
CVE-2024-38173	Microsoft Outlook Remote Code Execution Vulnerability	6.7	More Details
CVE-2024-42034	LaunchAnywhere vulnerability in the account module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	6.6	More Details
CVE-2022-27486	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiDDoS version 5.5.0 through 5.5.1, 5.4.2 through 5.4.0, 5.3.0 through 5.3.1, 5.2.0, 5.1.0, 5.0.0, 4.7.0, 4.6.0 and 4.5.0 and FortiDDoS-F version 6.3.0 through 6.3.1, 6.2.0 through 6.2.2, 6.1.0 through 6.1.4 allows an authenticated attacker to execute shell code as `root` via `execute` CLI commands.	6.6	More Details
CVE-2024-41903	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V2.0). The affected application mounts the container's root filesystem with read and write privileges. This could allow an attacker to alter the container's filesystem leading to unauthorized modifications and data corruption.	6.6	More Details
CVE-2023-28865	Diebold Nixdorf Vynamic Security Suite (VSS) before 3.3.0 SR15, 4.0.0 SR05, 4.1.0 SR03, and 4.2.0 SR02 fails to validate the directory contents of certain directories (e.g., ensuring the expected hash sum) during the Pre-Boot Authorization (PBA) process. This can be exploited by a physical attacker who is able to manipulate the contents of the system's hard disk.	6.6	More Details
CVE-2024-43231	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themeum Tutor LMS allows Stored XSS.This issue affects Tutor LMS: from n/a through 2.7.3.	6.5	More Details
CVE-2024-43151	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Brainstorm Force Ultimate Addons for Beaver Builder – Lite allows Stored XSS.This issue affects Ultimate Addons for Beaver Builder – Lite: from n/a through 1.5.9.	6.5	More Details
CVE-2024-5423	Multiple Denial of Service (DoS) conditions has been discovered in GitLab CE/EE affecting all versions starting from 1.0 prior to 17.0.6, starting from 17.1 prior to 17.1.4, and starting from 17.2 prior to 17.2.2 which allowed an attacker to cause resource exhaustion via banzai pipeline.	6.5	More Details
CVE-2024-43227	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPDeveloper BetterDocs allows Stored XSS.This issue affects BetterDocs: from n/a through 3.5.8.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38167	.NET and Visual Studio Information Disclosure Vulnerability	6.5	More Details
CVE-2024-7267	Exposure of Sensitive Information vulnerability in Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy EZD RP allows logged-in user to retrieve information about IP infrastructure and credentials. This issue affects EZD RP all versions before 19.6	6.5	More Details
CVE-2024-7700	A command injection flaw was found in the "Host Init Config" template in the Foreman application via the "Install Packages" field on the "Register Host" page. This flaw allows an attacker with the necessary privileges to inject arbitrary commands into the configuration, potentially allowing unauthorized command execution during host registration. Although this issue requires user interaction to execute injected commands, it poses a significant risk if an unsuspecting user runs the generated registration script.	6.5	More Details
CVE-2024-7477	A SQL injection vulnerability was found which could allow a command line interface (CLI) user with administrative privileges to execute arbitrary queries against the Avaya Aura System Manager database. Affected versions include 10.1.x.x and 10.2.x.x. Versions prior to 10.1 are end of manufacturer support.	6.5	More Details
CVE-2024-34788	An improper authentication vulnerability in web component of EPMM prior to 12.1.0.1 allows a remote malicious user to access potentially sensitive information	6.5	More Details
CVE-2024-43155	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PickPlugins ComboBlocks allows Stored XSS.This issue affects ComboBlocks: from n/a through 2.2.86.	6.5	More Details
CVE-2024-38197	Microsoft Teams for iOS Spoofing Vulnerability	6.5	More Details
CVE-2024-43165	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Rashid87 WPSection allows PHP Local File Inclusion.This issue affects WPSection: from n/a through 1.3.8.	6.5	More Details
CVE-2024-43138	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in MagePeople Team Event Manager for WooCommerce allows PHP Local File Inclusion.This issue affects Event Manager for WooCommerce: from n/a through 4.2.1.	6.5	More Details
CVE-2024-38213	Windows Mark of the Web Security Feature Bypass Vulnerability	6.5	More Details
CVE-2024-38214	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	6.5	More Details
CVE-2024-42368	OpenTelemetry, also known as OTel, is a vendor-neutral open source Observability framework for instrumenting, generating, collecting, and exporting telemetry data such as traces, metrics, and logs. The bearertokenauth extension's server authenticator performs a simple, non-constant time string comparison of the received & configured bearer tokens. This impacts anyone using the `bearertokenauth` server authenticator. Malicious clients with network access to the collector may perform a timing attack against a collector with this authenticator to guess the configured token, by iteratively sending tokens and comparing the response time. This would allow an attacker to introduce fabricated or bad data into the collector's telemetry pipeline. The observable timing vulnerability was fixed by using constant-time comparison in 0.107.0	6.5	More Details
CVE-2024-42474	Streamlit is a data oriented application development framework for python. Snowflake Streamlit open source addressed a security vulnerability via the static file sharing feature. Users of hosted Streamlit app(s) on Windows were vulnerable to a path traversal vulnerability when the static file sharing feature is enabled. An attacker could utilize the vulnerability to leak the password hash of the Windows user running Streamlit. The vulnerability was patched on Jul 25, 2024, as part of Streamlit open source version 1.37.0. The vulnerability only affects Windows.	6.5	More Details
CVE-2024-7590	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Brainstorm Force Spectra allows Stored XSS.This issue affects Spectra: from n/a through 2.14.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38165	Windows Compressed Folder Tampering Vulnerability	6.5	More Details
CVE-2024-43149	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CreativeMindsSolutions CM Tooltip Glossary allows Stored XSS.This issue affects CM Tooltip Glossary: from n/a through 4.3.7.	6.5	More Details
CVE-2024-43150	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Xpro Xpro Elementor Addons allows Stored XSS.This issue affects Xpro Elementor Addons: from n/a through 1.4.4.2.	6.5	More Details
CVE-2024-43164	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Blockspare allows Stored XSS.This issue affects Blockspare: from n/a through 3.2.0.	6.5	More Details
CVE-2024-43129	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in WPDeveloper BetterDocs allows PHP Local File Inclusion.This issue affects BetterDocs: from n/a through 3.5.8.	6.5	More Details
CVE-2024-42376	SAP Shared Service Framework does not perform necessary authorization check for an authenticated user, resulting in escalation of privileges. On successful exploitation, an attacker can cause a high impact on confidentiality of the application.	6.5	More Details
CVE-2024-43128	Improper Control of Generation of Code ('Code Injection') vulnerability in WC Product Table WooCommerce Product Table Lite allows Code Injection.This issue affects WooCommerce Product Table Lite: from n/a through 3.5.1.	6.5	More Details
CVE-2024-41332	Incorrect access control in the delete_category function of Sourcecodester Computer Laboratory Management System v1.0 allows authenticated attackers with low-level privileges to arbitrarily delete categories.	6.5	More Details
CVE-2024-38219	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	6.5	More Details
CVE-2024-38200	Microsoft Office Spoofing Vulnerability	6.5	More Details
CVE-2023-20591	Improper re-initialization of IOMMU during the DRTM event may permit an untrusted platform configuration to persist, allowing an attacker to read or modify hypervisor memory, potentially resulting in loss of confidentiality, integrity, and availability.	6.5	More Details
CVE-2024-39642	Authorization Bypass Through User-Controlled Key vulnerability in ThimPress LearnPress allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects LearnPress: from n/a through 4.2.6.8.2.	6.5	More Details
CVE-2024-41978	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.1), RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2) (All versions < V8.1), SCALANCE M804PB (6GK5804-0AP00-2AA2) (All versions < V8.1), SCALANCE M812-1 ADSL-Router family (All versions < V8.1), SCALANCE M816-1 ADSL-Router family (All versions < V8.1), SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) (All versions < V8.1), SCALANCE M874-2 (6GK5874-2AA00-2AA2) (All versions < V8.1), SCALANCE M874-3 (6GK5874-3AA00-2AA2) (All versions < V8.1), SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2) (All versions < V8.1), SCALANCE M876-3 (6GK5876-3AA02-2BA2) (All versions < V8.1), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.1), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.1), SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) (All versions < V8.1), SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) (All versions < V8.1), SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1) (All versions < V8.1), SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1) (All versions < V8.1), SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) (All versions < V8.1), SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1) (All versions < V8.1), SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1) (All versions < V8.1), SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1) (All versions < V8.1), SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) (All versions < V8.1), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.1), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All versions < V8.1), SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2) (All versions < V8.1). Affected devices insert sensitive information about the generation of 2FA tokens into log files. This could allow an authenticated remote attacker to forge 2FA tokens of other users.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4210	A Denial of Service (DoS) condition has been discovered in GitLab CE/EE affecting all versions starting with 12.6 before 17.0.6, 17.1 prior to 17.1.4, and 17.2 prior to 17.2.2. It is possible for an attacker to cause a denial of service using crafted adoc files.	6.5	More Details
CVE-2024-2800	ReDoS flaw in RefMatcher when matching branch names using wildcards in GitLab EE/CE affecting all versions from 11.3 prior to 17.0.6, 17.1 prior to 17.1.4, and 17.2 prior to 17.2.2 allows denial of service via Regex backtracking.	6.5	More Details
CVE-2024-21877	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability through a url parameter in Enphase IQ Gateway (formerly known as Envoy) allows File Manipulation. The endpoint requires authentication.This issue affects Envoy: from 4.x to 8.0 and < 8.2.4225.	6.5	More Details
CVE-2024-38752	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Zoho Campaigns allows Cross-Site Scripting (XSS).This issue affects Zoho Campaigns: from n/a through 2.0.8.	6.5	More Details
CVE-2024-4359	The Element Pack Elementor Addons (Header Footer, Template Library, Dynamic Grid & Carousel, Remote Arrows) plugin for WordPress is vulnerable to arbitrary file reads in all versions up to, and including, 5.7.2 via the SVG widget and a lack of sufficient file validation in the render_svg function. This makes it possible for authenticated attackers, with contributor-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	6.5	More Details
CVE-2024-42470	openHAB, a provider of open-source home automation software, has add-ons including the visualization add-on CometVisu. Several endpoints in versions prior to 4.2.1 of the CometVisu add-on of openHAB don't require authentication. This makes it possible for unauthenticated attackers to modify or to steal sensitive data. This issue may lead to sensitive information disclosure. Users should upgrade to version 4.2.1 of the CometVisu add-on of openHAB to receive a patch.	6.5	More Details
CVE-2024-43147	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Merkulove Selection Lite allows Stored XSS.This issue affects Selection Lite: from n/a through 1.11.	6.5	More Details
CVE-2024-43224	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Yuri Baranov YaMaps for WordPress allows Stored XSS.This issue affects YaMaps for WordPress: from n/a through 0.6.27.	6.5	More Details
CVE-2024-43225	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ThemeLooks Enter Addons allows Stored XSS.This issue affects Enter Addons: from n/a through 2.1.7.	6.5	More Details
CVE-2024-6758	Improper Privilege Management in Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments.	6.5	More Details
CVE-2024-41251	An Incorrect Access Control vulnerability was found in /smsa/admin_teacher_register_approval.php and /smsa/admin_teacher_register_approval_submit.php in Kashipara Responsive School Management System v3.2.0, which allows remote unauthenticated attackers to view and approve Teacher registration.	6.5	More Details
CVE-2024-7408	This vulnerability exists in Airveda Air Quality Monitor PM2.5 PM10 due to transmission of sensitive information in plain text during AP pairing mode. An attacker in close proximity could exploit this vulnerability by capturing Wi-Fi traffic of Airveda-AP. Successful exploitation of this vulnerability could allow the attacker to cause Evil Twin attack on the targeted system.	6.5	More Details
CVE-2024-43226	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jeroen Sormani WP Dashboard Notes allows Stored XSS.This issue affects WP Dashboard Notes: from n/a through 1.0.11.	6.5	More Details
CVE-2024-43218	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Mediavine Mediavine Control Panel allows Stored XSS.This issue affects Mediavine Control Panel: from n/a through 2.10.4.	6.5	More Details
CVE-2024-43123	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Techeshta Card Elements for Elementor allows Stored XSS.This issue affects Card Elements for Elementor: from n/a through 1.2.2.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43216	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Patrick Posner Filr – Secure document library allows Stored XSS.This issue affects Filr – Secure document library: from n/a through 1.2.4.	6.5	More Details
CVE-2024-43124	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Iqonic Design Graphina allows Stored XSS.This issue affects Graphina: from n/a through 1.8.10.	6.5	More Details
CVE-2024-43125	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Table Builder WP Table Builder – WordPress Table Plugin allows Stored XSS.This issue affects WP Table Builder – WordPress Table Plugin: from n/a through 1.4.15.	6.5	More Details
CVE-2024-43210	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in LA-Studio LA-Studio Element Kit for Elementor allows Stored XSS.This issue affects LA-Studio Element Kit for Elementor: from n/a through 1.3.9.2.	6.5	More Details
CVE-2024-43133	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themify Themify Shortcodes allows Stored XSS.This issue affects Themify Shortcodes: from n/a through 2.1.1.	6.5	More Details
CVE-2024-6133	The wp-cart-for-digital-products WordPress plugin before 8.5.6 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	6.5	More Details
CVE-2024-43139	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Antoine Hurkmans Football Pool allows Stored XSS.This issue affects Football Pool: from n/a through 2.11.9.	6.5	More Details
CVE-2024-41252	An Incorrect Access Control vulnerability was found in /smsa/admin_student_register_approval.php and /smsa/admin_student_register_approval_submit.php in Kashipara Responsive School Management System v3.2.0, which allows remote unauthenticated attackers to view and approve student registration.	6.5	More Details
CVE-2024-6639	The MDx theme for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'mdx_list_item' shortcode in all versions up to, and including, 2.0.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5226	The Fuse Social Floating Sidebar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the file upload functionality in all versions up to, and including, 5.4.10 due to insufficient validation of SVG files. 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-2024-4360	The Element Pack Elementor Addons (Header Footer, Template Library, Dynamic Grid & Carousel, Remote Arrows) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widgets in all versions up to, and including, 5.7.2 due to insufficient input sanitization and output escaping on user supplied attributes like 'title_tag'. 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-2024-5668	The Lightbox & Modal Popup WordPress Plugin – FooBox plugin for WordPress is vulnerable to DOM-based Stored Cross-Site Scripting via HTML data attributes in all versions up to, and including, 2.7.28 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-2024-7247	The Element Pack Elementor Addons (Header Footer, Template Library, Dynamic Grid & Carousel, Remote Arrows) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Custom Gallery and Countdown widgets in all versions up to, and including, 5.7.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-7092	The Essential Addons for Elementor – Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘no_more_items_text’ parameter in all versions up to, and including, 5.9.27 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-2024-7715	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240812. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument filter leads to command injection. It is possible to initiate the attack 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. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2024-33005	Due to the missing authorization checks in the local systems, the admin users of SAP Web Dispatcher, SAP NetWeaver Application Server (ABAP and Java), and SAP Content Server can impersonate other users and may perform some unintended actions. This could lead to a low impact on confidentiality and a high impact on the integrity and availability of the applications.	6.3	More Details
CVE-2024-7748	A vulnerability, which was classified as critical, has been found in SourceCodester Accounts Manager App 1.0. This issue affects some unknown processing of the file /endpoint/delete-account.php. The manipulation of the argument account 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-2024-7750	A vulnerability has been found in SourceCodester Clinics Patient Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /medicines.php. The manipulation of the argument medicine_name 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-2024-7667	A vulnerability, which was classified as critical, was found in SourceCodester Car Driving School Management System 1.0. This affects the function delete_users of the file User.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-7751	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /update_medicine.php. The manipulation of the argument hidden_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-2024-6640	In ICMPv6 Neighbor Discovery (ND), the ID is always 0. When pf is configured to allow ND and block incoming Echo Requests, a crafted Echo Request packet after a Neighbor Solicitation (NS) can trigger an Echo Reply. The packet has to come from the same host as the NS and have a zero as identifier to match the state created by the Neighbor Discovery and allow replies to be generated. ICMPv6 packets with identifier value of zero bypass firewall rules written on the assumption that the incoming packets are going to create a state in the state table.	6.3	More Details
CVE-2024-7640	A vulnerability, which was classified as critical, has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0. This issue affects some unknown processing of the file delete_register.php. The manipulation of the argument case_register_id 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-2024-7665	A vulnerability classified as critical was found in SourceCodester Car Driving School Management System 1.0. Affected by this vulnerability is an unknown functionality of the file manage_package.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-2024-7664	A vulnerability classified as critical has been found in SourceCodester Car Driving School Management System 1.0. Affected is an unknown function of the file view_details.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-7663	A vulnerability was found in SourceCodester Car Driving School Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file manage_user.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-7643	A vulnerability was found in SourceCodester Leads Manager Tool 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /endpoint/delete-leads.php of the component Delete Leads Handler. The manipulation of the argument leads 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-2024-7642	A vulnerability has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file activate_act.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 Number	Description	Base Score	Reference
CVE-2024-7641	A vulnerability, which was classified as critical, was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. Affected is an unknown function of the file deactivate_act.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-7639	A vulnerability classified as critical was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. This vulnerability affects unknown code of the file delete_act.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-7668	A vulnerability has been found in SourceCodester Car Driving School Management System 1.0 and classified as critical. This vulnerability affects the function delete_package of the file Master.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-43045	Jenkins 2.470 and earlier, LTS 2.452.3 and earlier does not perform a permission check in an HTTP endpoint, allowing attackers with Overall/Read permission to access other users' "My Views".	6.3	More Details
CVE-2024-7579	A vulnerability was found in Alien Technology ALR-F800 up to 19.10.24.00. It has been declared as critical. Affected by this vulnerability is the function popen of the file /var/www/cgi-bin/upgrade.cgi of the component File Name Handler. The manipulation of the argument uploadedFile leads to os command injection. 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.	6.3	More Details
CVE-2024-7638	A vulnerability classified as critical has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0. This affects an unknown part of the file delete_client.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-7580	A vulnerability was found in Alien Technology ALR-F800 up to 19.10.24.00. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/system.html. The manipulation of the argument uploadedFile with the input ;whoami leads to os command injection. 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.	6.3	More Details
CVE-2024-7272	A vulnerability, which was classified as critical, was found in FFmpeg up to 5.1.5. This affects the function fill_audiodata of the file /libswresample/swresample.c. The manipulation leads to heap-based buffer overflow. It is possible to initiate the attack remotely. This issue was fixed in version 6.0 by 9903ba28c28ab18dc7b7b6fb8571cc8b5caae1a6 but a backport for 5.1 was forgotten. The exploit has been disclosed to the public and may be used. Upgrading to version 5.1.6 and 6.0 9903ba28c28ab18dc7b7b6fb8571cc8b5caae1a6 is able to address this issue. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2024-42165	Insufficiently random values for generating activation token in FIWARE Keyrock <= 8.4 allow attackers to activate accounts of any user by predicting the token for the activation link.	6.3	More Details
CVE-2024-7666	A vulnerability, which was classified as critical, has been found in SourceCodester Car Driving School Management System 1.0. Affected by this issue is some unknown functionality of the file view_package.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2023-38018	IBM Aspera Shares 1.10.0 PL2 does not invalidate session after a password change which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 260574.	6.3	More Details
CVE-2024-7669	A vulnerability was found in SourceCodester Car Driving School Management System 1.0 and classified as critical. This issue affects the function delete_enrollment of the file Master.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-7676	A vulnerability was found in Sourcecodester Car Driving School Management System 1.0. It has been classified as critical. Affected is the function save_package of the file /classes/Master.php?f=save_package. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-7680	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been classified as critical. This affects an unknown part of the file /incedit.php?id=4. The manipulation of the argument id/inccat/desc/date/amount 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 Number	Description	Base Score	Reference
CVE-2024-34609	Improper access control in VoiceNoteService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background.	6.2	More Details
CVE-2024-42030	Access permission verification vulnerability in the content sharing pop-up module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	6.2	More Details
CVE-2024-34605	Improper access control in SamsungHealthService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background.	6.2	More Details
CVE-2024-34606	Improper access control in SmartThingsService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background.	6.2	More Details
CVE-2024-34607	Improper access control in SamsungNotesService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background.	6.2	More Details
CVE-2024-34608	Improper access control in PaymentManagerService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background.	6.2	More Details
CVE-2024-34604	Improper access control in LedCoverService prior to SMR Aug-2024 Release 1 allows local attackers to bypass restrictions on starting services from the background.	6.2	More Details
CVE-2024-41481	Typora before 1.9.3 Markdown editor has a cross-site scripting (XSS) vulnerability via the Mermaid component.	6.1	More Details
CVE-2024-40484	A Reflected Cross Site Scripting (XSS) vulnerability was found in "/oahms/search.php" in PHPGurukul Old Age Home Management System v1.0, which allows remote attackers to execute arbitrary code via the "searchdata" parameter.	6.1	More Details
CVE-2024-41482	Typora before 1.9.3 Markdown editor has a cross-site scripting (XSS) vulnerability via the MathJax component.	6.1	More Details
CVE-2024-6892	Attackers can craft a malicious link that once clicked will execute arbitrary JavaScript in the context of the Journyx web application.	6.1	More Details
CVE-2024-6706	Attackers can craft a malicious prompt that coerces the language model into executing arbitrary JavaScript in the context of the web page.	6.1	More Details
CVE-2024-41242	A Reflected Cross Site Scripting (XSS) vulnerability was found in /smsa/student_login.php in Kashipara Responsive School Management System v3.2.0, which allows remote attackers to execute arbitrary code via "error" parameter.	6.1	More Details
CVE-2024-41241	A Reflected Cross Site Scripting (XSS) vulnerability was found in " /smsa/admin_login.php" in Kashipara Responsive School Management System v3.2.0, which allows remote attackers to execute arbitrary code via "error" parameter.	6.1	More Details
CVE-2024-41240	A Reflected Cross Site Scripting (XSS) vulnerability was found in " /smsa/teacher_login.php" in Kashipara Responsive School Management System v3.2.0, which allows remote attackers to execute arbitrary code via the "error" parameter.	6.1	More Details
CVE-2024-27443	An issue was discovered in Zimbra Collaboration (ZCS) 9.0 and 10.0. A Cross-Site Scripting (XSS) vulnerability exists in the CalendarInvite feature of the Zimbra webmail classic user interface, because of improper input validation in the handling of the calendar header. An attacker can exploit this via an email message containing a crafted calendar header with an embedded XSS payload. When a victim views this message in the Zimbra webmail classic interface, the payload is executed in the context of the victim's session, potentially leading to execution of arbitrary JavaScript code.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43358	ZoneMinder is a free, open source closed-circuit television software application. ZoneMinder has a cross-site scripting vulnerability in the filter view via the filter[Id]. This vulnerability is fixed in 1.36.34 and 1.37.61.	6.1	More Details
CVE-2024-21550	SteVe is an open platform that implements different version of the OCPP protocol for Electric Vehicle charge points, acting as a central server for management of registered charge points. Attackers can inject arbitrary HTML and Javascript code via WebSockets leading to persistent Cross-Site Scripting in the SteVe management interface.	6.1	More Details
CVE-2024-21757	A unverified password change in Fortinet FortiManager versions 7.0.0 through 7.0.10, versions 7.2.0 through 7.2.4, and versions 7.4.0 through 7.4.1, as well as Fortinet FortiAnalyzer versions 7.0.0 through 7.0.10, versions 7.2.0 through 7.2.4, and versions 7.4.0 through 7.4.1, allows an attacker to modify admin passwords via the device configuration backup.	6.1	More Details
CVE-2024-38501	An unauthenticated remote attacker may use a HTML injection vulnerability with limited length to inject malicious HTML code and gain low-privileged access on the affected device.	6.1	More Details
CVE-2024-6494	The WordPress File Upload WordPress plugin before 4.24.8 does not properly sanitize and escape certain parameters, which could allow unauthenticated users to execute stored cross-site scripting (XSS) attacks.	6.1	More Details
CVE-2024-22121	A non-admin user can change or remove important features within the Zabbix Agent application, thus impacting the integrity and availability of the application.	6.1	More Details
CVE-2024-7649	The Opal Membership plugin for WordPress is vulnerable to Stored Cross-Site Scripting via checkout form fields in all versions up to, and including, 1.2.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.1	More Details
CVE-2024-0115	NVIDIA CV-CUDA for Ubuntu 20.04, Ubuntu 22.04, and Jetpack contains a vulnerability in Python APIs where a user may cause an uncontrolled resource consumption issue by a long running CV-CUDA Python process. A successful exploit of this vulnerability may lead to denial of service and data loss.	6.1	More Details
CVE-2024-7574	The Christmasify! plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.5.5. This is due to missing nonce validation on the 'options' function. This makes it possible for unauthenticated attackers to modify the plugin's settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2023-50810	In certain Sonos products before Sonos S1 Release 11.12 and S2 release 15.9, a vulnerability exists in the U-Boot component of the firmware that allow persistent arbitrary code execution with Linux kernel privileges. A failure to correctly handle the return value of the setenv command can be used to override the kernel command-line parameters and ultimately bypass the Secure Boot implementation. This affects PLAY5 gen 2, PLAYBASE, PLAY:1, One, One SL, and Amp.	6.0	More Details
CVE-2024-35775	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting'), Improper Authentication vulnerability in Soliloquy Team Slider by Soliloquy allows Cross-Site Scripting (XSS).This issue affects Slider by Soliloquy: from n/a through 2.7.6.	5.9	More Details
CVE-2024-43130	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Antoine Hurkmans Football Pool allows Stored XSS.This issue affects Football Pool: from n/a through 2.11.10.	5.9	More Details
CVE-2024-43137	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WappPress Team WappPress allows Stored XSS.This issue affects WappPress: from n/a through 6.0.4.	5.9	More Details
CVE-2024-43148	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in bPlugins StreamCast allows Stored XSS.This issue affects StreamCast: from n/a through 2.2.3.	5.9	More Details
CVE-2024-43152	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in iberezansky 3D FlipBook – PDF Flipbook Viewer, Flipbook Image Gallery allows Stored XSS.This issue affects 3D FlipBook – PDF Flipbook Viewer, Flipbook Image Gallery: from n/a through 1.15.6.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41909	Like many other SSH implementations, Apache MINA SSHD suffered from the issue that is more widely known as CVE-2023-48795. An attacker that can intercept traffic between client and server could drop certain packets from the stream, potentially causing client and server to consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack The mitigations to prevent this type of attack were implemented in Apache MINA SSHD 2.12.0, both client and server side. Users are recommended to upgrade to at least this version. Note that both the client and the server implementation must have mitigations applied against this issue, otherwise the connection may still be affected.	5.9	More Details
CVE-2024-43161	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Averta Depicter Slider allows Stored XSS.This issue affects Depicter Slider: from n/a through 3.1.2.	5.9	More Details
CVE-2024-21981	Improper key usage control in AMD Secure Processor (ASP) may allow an attacker with local access who has gained arbitrary code execution privilege in ASP to extract ASP cryptographic keys, potentially resulting in loss of confidentiality and integrity.	5.7	More Details
CVE-2024-6329	An issue was discovered in GitLab CE/EE affecting all versions starting from 8.16 prior to 17.0.6, starting from 17.1 prior to 17.1.4, and starting from 17.2 prior to 17.2.2, which causes the web interface to fail to render the diff correctly when the path is encoded.	5.7	More Details
CVE-2021-26367	A malicious attacker in x86 can misconfigure the Trusted Memory Regions (TMRs), which may allow the attacker to set an arbitrary address range for the TMR, potentially leading to a loss of integrity and availability.	5.7	More Details
CVE-2024-42243	In the Linux kernel, the following vulnerability has been resolved: mm/filemap: make MAX_PAGECACHE_ORDER acceptable to xarray Patch series "mm/filemap: Limit page cache size to that supported by xarray", v2. Currently, xarray can't support arbitrary page cache size. More details can be found from the WARN_ON() statement in xas_split_alloc(). In our test whose code is attached below, we hit the WARN_ON() on ARM64 system where the base page size is 64KB and huge page size is 512MB. The issue was reported long time ago and some discussions on it can be found here [1]. [1] https://www.spinics.net/lists/linux-xfs/msg75404.html In order to fix the issue, we need to adjust MAX_PAGECACHE_ORDER to one supported by xarray and avoid PMD-sized page cache if needed. The code changes are suggested by David Hildenbrand. PATCH[1] adjusts MAX_PAGECACHE_ORDER to that supported by xarray PATCH[2-3] avoids PMD-sized page cache in the synchronous readahead path PATCH[4] avoids PMD-sized page cache for shmem files if needed Test program ========== # cat test.c #define _GNU_SOURCE #include <stdio.h> #include <stdlib.h> #include <unistd.h> #include <string.h> #include <fcntl.h> #include <errno.h> #include <sys/syscall.h> #include <sys/mman.h> #define TEST_XFS_FILENAME "/tmp/data" #define TEST_SHMEM_FILENAME "/dev/shm/data" #define TEST_MEM_SIZE 0x20000000 int main(int argc, char **argv) { const char *filename; int fd = 0; void *buf = (void *)-1, *p; int pgsize = getpagesize(); int ret; if (pgsize != 0x10000) { fprintf(stderr, "64KB base page size is required\n"); return -EPERM; } system("echo force > /sys/kernel/mm/transparent_hugepage/shmem_enabled"); system("rm -fr /tmp/data"); system("rm -fr /dev/shm/data"); system("echo 1 > /proc/sys/vm/drop_caches"); /* Open xfs or shmem file */ filename = TEST_XFS_FILENAME; if (argc > 1 && !strcmp(argv[1], "shmem")) filename = TEST_SHMEM_FILENAME; fd = open(filename, O_CREAT | O_RDWR | O_TRUNC); if (fd < 0) { fprintf(stderr, "Unable to open <%s>\n", filename); return -EIO; } /* Extend file size */ ret = ftruncate(fd, TEST_MEM_SIZE); if (ret) { fprintf(stderr, "Error %d to ftruncate()\n", ret); goto cleanup; } /* Create VMA */ buf = mmap(NULL, TEST_MEM_SIZE, PROT_READ | PROT_WRITE, MAP_SHARED, fd, 0); if (buf == (void *)-1) { fprintf(stderr, "Unable to mmap <%s>\n", filename); goto cleanup; } fprintf(stdout, "mapped buffer at 0x%p\n", buf); ret = madvise(buf, TEST_MEM_SIZE, MADV_HUGEPAGE); if (ret) { fprintf(stderr, "Unable to madvise(MADV_HUGEPAGE)\n"); goto cleanup; } /* Populate VMA */ ret = madvise(buf, TEST_MEM_SIZE, MADV_POPULATE_WRITE); if (ret) { fprintf(stderr, "Error %d to madvise(MADV_POPULATE_WRITE)\n", ret); goto cleanup; } /* Punch the file to enforce xarray split */ ret = fallocate(fd, FALLOC_FL_KEEP_SIZE | FALLOC_FL_PUNCH_HOLE, TEST_MEM_SIZE - pgsize, pgsize); if (ret) fprintf(stderr, "Error %d to fallocate()\n", ret); cleanup: if (buf != (void *)-1) munmap(buf, TEST_MEM_SIZE); if (fd > 0) close(fd); return 0; } # gcc test.c -o test # cat /proc/1/smaps | grep KernelPageSize | head -n 1 KernelPageSize: 64 kB # ./test shmem : ------------[cut here]------------ WARNING: CPU: 17 PID: 5253 at lib/xarray.c:1025 xas_split_alloc+0xf8/0x128 Modules linked in: nft_fib_inet nft_fib_ipv4 nft_fib_ipv6 nft_fib \ nft_reject_inet nf_reject_ipv4 nf_reject_ipv6 nft_reject nft_ct \ nft_chain_nat nf_nat nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 \ ip_set nf_tables rfkill nfnetlink vfat fat virtio_balloon \ drm fuse xfs libcrc32c crct10dif_ce ghash_ce sha2_ce sha256_arm64 \ virtio_net sha1_ce net_failover failover virtio_console virtio_blk \ dimlib virtio_mmio CPU: 17 PID: 5253 Comm: test Kdump: loaded Tainted: G W 6.10.0-rc5-gavin+ #12 Hardware name: QEMU KVM Virtual Machine, BIOS edk2-20240524-1.el9 05/24/2024 pstate: 83400005 (Nzcv daif +PAN -UAO +TC ---truncated---	5.5	More Details
CVE-2024-41938	A vulnerability has been identified in SINEC NMS (All versions < V3.0). The importCertificate function of the SINEC NMS Control web application contains a path traversal vulnerability. This could allow an authenticated attacker it to delete arbitrary certificate files on the drive SINEC NMS is installed on.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42245	In the Linux kernel, the following vulnerability has been resolved: Revert "sched/fair: Make sure to try to detach at least one movable task" This reverts commit b0defa7ae03ecf91b8bfd10ede430cff12fcbd06. b0defa7ae03ec changed the load balancing logic to ignore env.max_loop if all tasks examined to that point were pinned. The goal of the patch was to make it more likely to be able to detach a task buried in a long list of pinned tasks. However, this has the unfortunate side effect of creating an O(n) iteration in detach_tasks(), as we now must fully iterate every task on a cpu if all or most are pinned. Since this load balance code is done with rq lock held, and often in softirq context, it is very easy to trigger hard lockups. We observed such hard lockups with a user who affined O(10k) threads to a single cpu. When I discussed this with Vincent he initially suggested that we keep the limit on the number of tasks to detach, but increase the number of tasks we can search. However, after some back and forth on the mailing list, he recommended we instead revert the original patch, as it seems likely no one was actually getting hit by the original issue.	5.5	More Details
CVE-2024-42246	In the Linux kernel, the following vulnerability has been resolved: net, sunrpc: Remap EPERM in case of connection failure in xs_tcp_setup_socket When using a BPF program on kernel_connect(), the call can return -EPERM. This causes xs_tcp_setup_socket() to loop forever, filling up the syslog and causing the kernel to potentially freeze up. Neil suggested: This will propagate -EPERM up into other layers which might not be ready to handle it. It might be safer to map EPERM to an error we would be more likely to expect from the network system - such as ECONNREFUSED or ENETDOWN. ECONNREFUSED as error seems reasonable. For programs setting a different error can be out of reach (see handling in 4fbac77d2d09) in particular on kernels which do not have f10d05966196 ("bpf: Make BPF_PROG_RUN_ARRAY return -err instead of allow boolean"), thus given that it is better to simply remap for consistent behavior. UDP does handle EPERM in xs_udp_send_request().	5.5	More Details
CVE-2024-42255	In the Linux kernel, the following vulnerability has been resolved: tpm: Use auth only after NULL check in tpm_buf_check_hmac_response() Dereference auth after NULL check in tpm_buf_check_hmac_response(). Otherwise, unless tpm2_sessions_init() was called, a call can cause NULL dereference, when TCG_TPM2_HMAC is enabled. [jarkko: adjusted the commit message.]	5.5	More Details
CVE-2024-34630	Out-of-bounds read in applying own binary with textbox in Samsung Notes prior to version 4.4.21.62 allows local attackers to potentially read memory.	5.5	More Details
CVE-2024-42248	In the Linux kernel, the following vulnerability has been resolved: tty: serial: ma35d1: Add a NULL check for of_node The pdev->dev.of_node can be NULL if the "serial" node is absent. Add a NULL check to return an error in such cases.	5.5	More Details
CVE-2024-42250	In the Linux kernel, the following vulnerability has been resolved: cachefiles: add missing lock protection when polling Add missing lock protection in poll routine when iterating xarray, otherwise: Even with RCU read lock held, only the slot of the radix tree is ensured to be pinned there, while the data structure (e.g. struct cachefiles_req) stored in the slot has no such guarantee. The poll routine will iterate the radix tree and dereference cachefiles_req accordingly. Thus RCU read lock is not adequate in this case and spinlock is needed here.	5.5	More Details
CVE-2024-7061	Okta Verify for Windows is vulnerable to privilege escalation through DLL hijacking. The vulnerability is fixed in Okta Verify for Windows version 5.0.2. To remediate this vulnerability, upgrade to 5.0.2 or greater.	5.5	More Details
CVE-2024-38122	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability	5.5	More Details
CVE-2024-38118	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability	5.5	More Details
CVE-2024-42254	In the Linux kernel, the following vulnerability has been resolved: io_uring: fix error pbuf checking Syz reports a problem, which boils down to NULL vs IS_ERR inconsistent error handling in io_alloc_pbuf_ring(). KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007] RIP: 0010:__io_remove_buffers+0xac/0x700 io_uring/kbuf.c:341 Call Trace: <TASK> io_put_bl io_uring/kbuf.c:378 [inline] io_destroy_buffers+0x14e/0x490 io_uring/kbuf.c:392 io_ring_ctx_free+0xa00/0x1070 io_uring/io_uring.c:2613 io_ring_exit_work+0x80f/0x8a0 io_uring/io_uring.c:2844 process_one_work kernel/workqueue.c:3231 [inline] process_scheduled_works+0xa2c/0x1830 kernel/workqueue.c:3312 worker_thread+0x86d/0xd40 kernel/workqueue.c:3390 kthread+0x2f0/0x390 kernel/kthread.c:389 ret_from_fork+0x4b/0x80 arch/x86/kernel/process.c:147 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:244	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42258	In the Linux kernel, the following vulnerability has been resolved: mm: huge_memory: use !CONFIG_64BIT to relax huge page alignment on 32 bit machines Yves-Alexis Perez reported commit 4ef9ad19e176 ("mm: huge_memory: don't force huge page alignment on 32 bit") didn't work for x86_32 [1]. It is because x86_32 uses CONFIG_X86_32 instead of CONFIG_32BIT. !CONFIG_64BIT should cover all 32 bit machines. [1] https://lore.kernel.org/linux-mm/CAHbLzkr1LwH3pcTgM+aGQ31ip2bKqiqEQ8=FQB+t2c3dhNKNHA@mail.gmail.com/	5.5	More Details
CVE-2024-42252	In the Linux kernel, the following vulnerability has been resolved: closures: Change BUG_ON() to WARN_ON() If a BUG_ON() can be hit in the wild, it shouldn't be a BUG_ON() For reference, this has popped up once in the CI, and we'll need more info to debug it: 03240 ------------[cut here]------------ 03240 kernel BUG at lib/closure.c:21! 03240 kernel BUG at lib/closure.c:21! 03240 Internal error: Oops - BUG: 00000000f2000800 [#1] SMP 03240 Modules linked in: 03240 CPU: 15 PID: 40534 Comm: kworker/u80:1 Not tainted 6.10.0-rc4-ktest-ga56da69799bd #25570 03240 Hardware name: linux,dummy-virt (DT) 03240 Workqueue: btree_update btree_interior_update_work 03240 pstate: 00001005 (nzcv daif -PAN -UAO -TCO -DIT +SSBS BTYPE=--) 03240 pc : closure_put+0x224/0x2a0 03240 lr : closure_put+0x24/0x2a0 03240 sp : ffff0000d12071c0 03240 x29: ffff0000d12071c0 x28: dfff800000000000 x27: ffff0000d1207360 03240 x26: 0000000000000040 x25: 0000000000000040 x24: 0000000000000040 03240 x23: ffff0000c1f20180 x22: 0000000000000000 x21: ffff0000c1f20168 03240 x20: 0000000040000000 x19: ffff0000c1f20140 x18: 0000000000000001 03240 x17: 0000000000003aa0 x16: 0000000000003ad0 x15: 1fffe0001c326974 03240 x14: 0000000000000a1e x13: 0000000000000000 x12: 1fffe000183e402d 03240 x11: ffff6000183e402d x10: dfff800000000000 x9 : ffff6000183e402e 03240 x8 : 0000000000000001 x7 : 00009fffe7c1bfd3 x6 : ffff0000c1f2016b 03240 x5 : ffff0000c1f20168 x4 : ffff6000183e402e x3 : ffff800081391954 03240 x2 : 0000000000000001 x1 : 0000000000000000 x0 : 00000000a8000000 03240 Call trace: 03240 closure_put+0x224/0x2a0 03240 bch2_check_for_deadlock+0x910/0x1028 03240 bch2_six_check_for_deadlock+0x1c/0x30 03240 six_lock_slowpath.isra.0+0x29c/0xed0 03240 six_lock_ip_waiter+0xa8/0xf8 03240 __bch2_btree_node_lock_write+0x14c/0x298 03240 bch2_trans_lock_write+0x6d4/0xb10 03240 __bch2_trans_commit+0x135c/0x5520 03240 btree_interior_update_work+0x1248/0x1c10 03240 process_scheduled_works+0x53c/0xd90 03240 worker_thread+0x370/0x8c8 03240 kthread+0x258/0x2e8 03240 ret_from_fork+0x10/0x20 03240 Code: aa1303e0 d63f0020 a94363f7 17ffff8c (d4210000) 03240 ---[end trace 0000000000000000]--- 03240 Kernel panic - not syncing: Oops - BUG: Fatal exception 03240 SMP: stopping secondary CPUs 03241 SMP: failed to stop secondary CPUs 13,15 03241 Kernel Offset: disabled 03241 CPU features: 0x00,00000003,80000008,4240500b 03241 Memory Limit: none 03241 ---[end Kernel panic - not syncing: Oops - BUG: Fatal exception]--- 03246 ========== FAILED TIMEOUT copygc_torture_no_checksum in 7200s	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42251	In the Linux kernel, the following vulnerability has been resolved: mm: page_ref: remove folio_try_get_rcu() The below bug was reported on a non-SMP kernel: [275.267158][T4335] ------------[cut here]------------ [275.267949][T4335] kernel BUG at include/linux/page_ref.h:275! [275.268526][T4335] invalid opcode: 0000 [#1] KASAN PTI [275.269001][T4335] CPU: 0 PID: 4335 Comm: trinity-c3 Not tainted 6.7.0-rc4-00061-gefa7df3e3bb5 #1 [275.269787][T4335] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.2-debian-1.16.2-1 04/01/2014 [275.270679][T4335] RIP: 0010:try_get_folio (include/linux/page_ref.h:275 (discriminator 3) mm/gup.c:79 (discriminator 3)) [275.272813][T4335] RSP: 0018:ffffc90005dcf650 EFLAGS: 00010202 [275.273346][T4335] RAX: 0000000000000246 RBX: ffffea00066e0000 RCX: 0000000000000000 [275.274032][T4335] RDX: fffff94000cdc007 RSI: 0000000000000004 RDI: ffffea00066e0034 [275.274719][T4335] RBP: ffffea00066e0000 R08: 0000000000000000 R09: fffff94000cdc006 [275.275404][T4335] R10: ffffea00066e0037 R11: 0000000000000000 R12: 0000000000000136 [275.276106][T4335] R13: ffffea00066e0034 R14: dfffffc0000000000 R15: ffffea00066e0008 [275.276790][T4335] FS: 00007fa2f9b61740(0000) GS:ffffffff89d0d000(0000) knlGS:0000000000000000 [275.277570][T4335] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [275.278143][T4335] CR2: 00007fa2f6c00000 CR3: 0000000134b04000 CR4: 00000000000406f0 [275.278833][T4335] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [275.279521][T4335] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [275.280201][T4335] Call Trace: [275.280499][T4335] <TASK> [275.280751][T4335] ? die (arch/x86/kernel/dumpstack.c:421 arch/x86/kernel/dumpstack.c:434 arch/x86/kernel/dumpstack.c:447) [275.281087][T4335] ? do_trap (arch/x86/kernel/traps.c:112 arch/x86/kernel/traps.c:153) [275.281463][T4335] ? try_get_folio (include/linux/page_ref.h:275 (discriminator 3) mm/gup.c:79 (discriminator 3)) [275.281884][T4335] ? try_get_folio (include/linux/page_ref.h:275 (discriminator 3) mm/gup.c:79 (discriminator 3)) [275.282300][T4335] ? do_error_trap (arch/x86/kernel/traps.c:174) [275.282711][T4335] ? try_get_folio (include/linux/page_ref.h:275 (discriminator 3) mm/gup.c:79 (discriminator 3)) [275.283129][T4335] ? handle_invalid_op (arch/x86/kernel/traps.c:212) [275.283561][T4335] ? try_get_folio (include/linux/page_ref.h:275 (discriminator 3) mm/gup.c:79 (discriminator 3)) [275.283990][T4335] ? exc_invalid_op (arch/x86/kernel/traps.c:264) [275.284415][T4335] ? asm_exc_invalid_op (arch/x86/include/asm/idtentry.h:568) [275.284859][T4335] ? try_get_folio (include/linux/page_ref.h:275 (discriminator 3) mm/gup.c:79 (discriminator 3)) [275.285278][T4335] try_grab_folio (mm/gup.c:148) [275.285684][T4335] __get_user_pages (mm/gup.c:1297 (discriminator 1)) [275.286111][T4335] ? __pfx___get_user_pages (mm/gup.c:1188) [275.286579][T4335] ? __pfx_validate_chain (kernel/locking/lockdep.c:3825) [275.287034][T4335] ? mark_lock (kernel/locking/lockdep.c:4656 (discriminator 1)) [275.287416][T4335] __gup_longterm_locked (mm/gup.c:1509 mm/gup.c:2209) [275.288192][T4335] ? __pfx___gup_longterm_locked (mm/gup.c:2204) [275.288697][T4335] ? __pfx_lock_acquire (kernel/locking/lockdep.c:5722) [275.289135][T4335] ? __pfx___might_resched (kernel/sched/core.c:10106) [275.289595][T4335] pin_user_pages_remote (mm/gup.c:3350) [275.290041][T4335] ? __pfx_pin_user_pages_remote (mm/gup.c:3350) [275.290545][T4335] ? find_held_lock (kernel/locking/lockdep.c:5244 (discriminator 1)) [275.290961][T4335] ? mm_access (kernel/fork.c:1573) [275.291353][T4335] process_vm_rw_single_vec+0x142/0x360 [275.291900][T4335] ? __pfx_process_vm_rw_single_vec+0x10/0x10 [275.292471][T4335] ? mm_access (kernel/fork.c:1573) [275.292859][T4335] process_vm_rw_core+0x272/0x4e0 [275.293384][T4335] ? hlock_class (a ---truncated---	5.5	More Details
CVE-2024-34624	Out-of-bounds read in applying paragraphs in Samsung Notes prior to version 4.4.21.62 allows local attackers to potentially read memory.	5.5	More Details
CVE-2024-42244	In the Linux kernel, the following vulnerability has been resolved: USB: serial: mos7840: fix crash on resume Since commit c49cfa917025 ("USB: serial: use generic method if no alternative is provided in usb serial layer"), USB serial core calls the generic resume implementation when the driver has not provided one. This can trigger a crash on resume with mos7840 since support for multiple read URBs was added back in 2011. Specifically, both port read URBs are now submitted on resume for open ports, but the context pointer of the second URB is left set to the core rather than mos7840 port structure. Fix this by implementing dedicated suspend and resume functions for mos7840. Tested with Delock 87414 USB 2.0 to 4x serial adapter. [johan: analyse crash and rewrite commit message; set busy flag on resume; drop bulk-in check; drop unnecessary usb_kill_urb()]	5.5	More Details
CVE-2024-34629	Out-of-bounds read in applying binary with text common object in Samsung Notes prior to version 4.4.21.62 allows local attackers to potentially read memory.	5.5	More Details
CVE-2024-34621	Out-of-bounds read in applying binary with data in Samsung Notes prior to version 4.4.21.62 allows local attackers to potentially read memory.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42236	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: configfs: Prevent OOB read/write in usb_string_copy() Userspace provided string 's' could trivially have the length zero. Left unchecked this will firstly result in an OOB read in the form `if (str[0 - 1] == '\n') followed closely by an OOB write in the form `str[0 - 1] = '\0'`. There is already a validating check to catch strings that are too long. Let's supply an additional check for invalid strings that are too short.	5.5	More Details
CVE-2024-34631	Out-of-bounds read in applying new binary in Samsung Notes prior to version 4.4.21.62 allows local attackers to potentially read memory.	5.5	More Details
CVE-2024-37403	Ivanti Docs@Work for Android, before 2.26.0 is affected by the 'Dirty Stream' vulnerability. The application fails to properly sanitize file names, resulting in a path traversal-affiliated vulnerability. This potentially enables other malicious apps on the device to read sensitive information stored in the app root.	5.5	More Details
CVE-2024-34628	Out-of-bounds read in applying binary with path in Samsung Notes prior to version 4.4.21.62 allows local attackers to potentially read memory.	5.5	More Details
CVE-2024-34627	Out-of-bounds read in parsing implemention in Samsung Notes prior to version 4.4.21.62 allows local attackers to potentially read memory.	5.5	More Details
CVE-2024-34626	Out-of-bounds read in applying own binary in Samsung Notes prior to version 4.4.21.62 allows local attackers to potentially read memory.	5.5	More Details
CVE-2024-34625	Out-of-bounds read in applying connection point in Samsung Notes prior to version 4.4.21.62 allows local attackers to potentially read memory.	5.5	More Details
CVE-2024-7616	A vulnerability was found in Edimax IC-6220DC and IC-5150W up to 3.06. It has been rated as critical. Affected by this issue is the function cgiFormString of the file ipcam_cgi. The manipulation of the argument host leads to command injection. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2024-42242	In the Linux kernel, the following vulnerability has been resolved: mmc: sdhci: Fix max_seg_size for 64KiB PAGE_SIZE blk_queue_max_segment_size() ensured: if (max_size < PAGE_SIZE) max_size = PAGE_SIZE; whereas: blk_validate_limits() makes it an error: if (WARN_ON_ONCE(lim->max_segment_size < PAGE_SIZE)) return -EINVAL; The change from one to the other, exposed sdhci which was setting maximum segment size too low in some circumstances. Fix the maximum segment size when it is too low.	5.5	More Details
CVE-2024-38155	Security Center Broker Information Disclosure Vulnerability	5.5	More Details
CVE-2024-42232	In the Linux kernel, the following vulnerability has been resolved: libceph: fix race between delayed_work() and ceph_monc_stop() The way the delayed work is handled in ceph_monc_stop() is prone to races with mon_fault() and possibly also finish_hunting(). Both of these can requeue the delayed work which wouldn't be canceled by any of the following code in case that happens after cancel_delayed_work_sync() runs -- __close_session() doesn't mess with the delayed work in order to avoid interfering with the hunting interval logic. This part was missed in commit b5d91704f53e ("libceph: behave in mon_fault() if cur_mon < 0") and use-after-free can still ensue on monc and objects that hang off of it, with monc->auth and monc->monmap being particularly susceptible to quickly being reused. To fix this: - clear monc->cur_mon and monc->hunting as part of closing the session in ceph_monc_stop() - bail from delayed_work() if monc->cur_mon is cleared, similar to how it's done in mon_fault() and finish_hunting() (based on monc->hunting) - call cancel_delayed_work_sync() after the session is closed	5.5	More Details
CVE-2024-38151	Windows Kernel Information Disclosure Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42234	In the Linux kernel, the following vulnerability has been resolved: mm: fix crashes from deferred split racing folio migration Even on 6.10-rc6, I've been seeing elusive "Bad page state"s (often on flags when freeing, yet the flags shown are not bad: PG_locked had been set and cleared??), and VM_BUG_ON_PAGE(page_ref_count(page) == 0)s from deferred_split_scan()'s folio_put(), and a variety of other BUG and WARN symptoms implying double free by deferred split and large folio migration. 6.7 commit 9bcef5973e31 ("mm: memcg: fix split queue list crash when large folio migration") was right to fix the memcg-dependent locking broken in 85ce2c517ade ("memcontrol: only transfer the memcg data for migration"), but missed a subtlety of deferred_split_scan(): it moves folios to its own local list to work on them without split_queue_lock, during which time folio->_deferred_list is not empty, but even the "right" lock does nothing to secure the folio and the list it is on. Fortunately, deferred_split_scan() is careful to use folio_try_get(): so folio_migrate_mapping() can avoid the race by folio_undo_large_rmappable() while the old folio's reference count is temporarily frozen to 0 - adding such a freeze in the !mapping case too (originally, folio lock and unmapping and no swap cache left an anon folio unreachable, so no freezing was needed there: but the deferred split queue offers a way to reach it).	5.5	More Details
CVE-2024-42235	In the Linux kernel, the following vulnerability has been resolved: s390/mm: Add NULL pointer check to crst_table_free() base_crst_free() crst_table_free() used to work with NULL pointers before the conversion to ptdescs. Since crst_table_free() can be called with a NULL pointer (error handling in crst_table_upgrade() add an explicit check. Also add the same check to base_crst_free() for consistency reasons. In real life this should not happen, since order two GFP_KERNEL allocations will not fail, unless FAIL_PAGE_ALLOC is enabled and used.	5.5	More Details
CVE-2024-42247	In the Linux kernel, the following vulnerability has been resolved: wireguard: allowedips: avoid unaligned 64-bit memory accesses On the parisc platform, the kernel issues kernel warnings because swap_endian() tries to load a 128-bit IPv6 address from an unaligned memory location: Kernel: unaligned access to 0x55f4688c in wg_allowedips_insert_v6+0x2c/0x80 [wireguard] (iir 0xf3010df) Kernel: unaligned access to 0x55f46884 in wg_allowedips_insert_v6+0x38/0x80 [wireguard] (iir 0xf2010dc) Avoid such unaligned memory accesses by instead using the get_unaligned_be64() helper macro. [Jason: replace src[8] in original patch with src+8]	5.5	More Details
CVE-2024-42241	In the Linux kernel, the following vulnerability has been resolved: mm/shmem: disable PMD-sized page cache if needed For shmem files, it's possible that PMD-sized page cache can't be supported by xarray. For example, 512MB page cache on ARM64 when the base page size is 64KB can't be supported by xarray. It leads to errors as the following messages indicate when this sort of xarray entry is split. WARNING: CPU: 34 PID: 7578 at lib/xarray.c:1025 xas_split_alloc+0xf8/0x128 Modules linked in: binfmt_misc nft_fib_inet nft_fib_ipv4 nft_fib_ipv6 \ nft_fib nft_reject_inet nf_reject_ipv4 nf_reject_ipv6 nft_reject \ nft_ct nft_chain_nat nf_nat nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 \ ip_set rfkill nf_tables nfnetlink vfat fat virtio_balloon drm fuse xfs \ libcrc32c crct10dif_ce ghash_ce sha2_ce sha256_arm64 sha1_ce virtio_net \ net_failover virtio_console virtio_blk failover dimlib virtio_mmio CPU: 34 PID: 7578 Comm: test Kdump: loaded Tainted: G W 6.10.0-rc5-gavin+ #9 Hardware name: QEMU KVM Virtual Machine, BIOS edk2-20240524-1.el9 05/24/2024 pstate: 83400005 (Nzcv daif +PAN -UAO +TCO +DIT -SSBS BTYPE=--) pc : xas_split_alloc+0xf8/0x128 lr : split_huge_page_to_list_to_order+0x1c4/0x720 sp : ffff8000882af5f0 x29: ffff8000882af5f0 x28: ffff8000882af650 x27: ffff8000882af768 x26: 0000000000000cc0 x25: 000000000000000d x24: ffff00010625b858 x23: ffff8000882af650 x22: fffffdfc0900000 x21: 0000000000000000 x20: 0000000000000000 x19: fffffdfc0900000 x18: 0000000000000000 x17: 0000000000000000 x16: 0000018000000000 x15: 52f8004000000000 x14: 0000e00000000000 x13: 0000000000002000 x12: 0000000000000020 x11: 52f8000000000000 x10: 52f8e1c0ffff6000 x9 : ffffbeb9619a681c x8 : 0000000000000003 x7 : 0000000000000000 x6 : ffff00010b02ddb0 x5 : ffffbeb96395e378 x4 : 0000000000000000 x3 : 0000000000000cc0 x2 : 000000000000000d x1 : 000000000000000c x0 : 0000000000000000 Call trace: xas_split_alloc+0xf8/0x128 split_huge_page_to_list_to_order+0x1c4/0x720 truncate_inode_partial_folio+0xdc/0x160 shmem_undo_range+0x2bc/0x6a8 shmem_fallocate+0x134/0x430 vfs_fallocate+0x124/0x2e8 ksys_fallocate+0x4c/0xa0 __arm64_sys_fallocate+0x24/0x38 invoke_syscall.constprop.0+0x7c/0xd8 do_el0_svc+0xb4/0xd0 el0_svc+0x44/0x1d8 el0t_64_sync_handler+0x134/0x150 el0t_64_sync+0x17c/0x180 Fix it by disabling PMD-sized page cache when HPAGE_PMD_ORDER is larger than MAX_PAGECACHE_ORDER. As Matthew Wilcox pointed, the page cache in a shmem file isn't represented by a multi-index entry and doesn't have this limitation when the xarry entry is split until commit 6b24ca4a1a8d ("mm: Use multi-index entries in the page cache").	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42240	In the Linux kernel, the following vulnerability has been resolved: x86/bhi: Avoid warning in #DB handler due to BHI mitigation When BHI mitigation is enabled, if SYSENTER is invoked with the TF flag set then entry_SYSENTER_compat() uses CLEAR_BRANCH_HISTORY and calls the clear_bhb_loop() before the TF flag is cleared. This causes the #DB handler (exc_debug_kernel()) to issue a warning because single-step is used outside the entry_SYSENTER_compat() function. To address this issue, entry_SYSENTER_compat() should use CLEAR_BRANCH_HISTORY after making sure the TF flag is cleared. The problem can be reproduced with the following sequence: $ cat sysenter_step.c int main() { asm("pushf; pop %ax; bts $8,%ax; push %ax; popf; sysenter"); } $ gcc -o sysenter_step sysenter_step.c $ ./sysenter_step Segmentation fault (core dumped) The program is expected to crash, and the #DB handler will issue a warning. Kernel log: WARNING: CPU: 27 PID: 7000 at arch/x86/kernel/traps.c:1009 exc_debug_kernel+0xd2/0x160 ... RIP: 0010:exc_debug_kernel+0xd2/0x160 ... Call Trace: <#DB> ? show_regs+0x68/0x80 ? __warn+0x8c/0x140 ? exc_debug_kernel+0xd2/0x160 ? report_bug+0x175/0x1a0 ? handle_bug+0x44/0x90 ? exc_invalid_op+0x1c/0x70 ? asm_exc_invalid_op+0x1f/0x30 ? exc_debug_kernel+0xd2/0x160 exc_debug+0x43/0x50 asm_exc_debug+0x1e/0x40 RIP: 0010:clear_bhb_loop+0x0/0xb0 ... </#DB> <TASK> ? entry_SYSENTER_compat_after_hwframe+0x6e/0x8d </TASK> [bp: Massage commit message.]	5.5	More Details
CVE-2024-42239	In the Linux kernel, the following vulnerability has been resolved: bpf: Fail bpf_timer_cancel when callback is being cancelled Given a schedule: timer1 cb timer2 cb bpf_timer_cancel(timer2); bpf_timer_cancel(timer1); Both bpf_timer_cancel calls would wait for the other callback to finish executing, introducing a lockup. Add an atomic_t count named 'cancelling' in bpf_hrtimer. This keeps track of all in-flight cancellation requests for a given BPF timer. Whenever cancelling a BPF timer, we must check if we have outstanding cancellation requests, and if so, we must fail the operation with an error (-EDEADLK) since cancellation is synchronous and waits for the callback to finish executing. This implies that we can enter a deadlock situation involving two or more timer callbacks executing in parallel and attempting to cancel one another. Note that we avoid incrementing the cancelling counter for the target timer (the one being cancelled) if bpf_timer_cancel is not invoked from a callback, to avoid spurious errors. The whole point of detecting cur->cancelling and returning -EDEADLK is to not enter a busy wait loop (which may or may not lead to a lockup). This does not apply in case the caller is in a non-callback context, the other side can continue to cancel as it sees fit without running into errors. Background on prior attempts: Earlier versions of this patch used a bool 'cancelling' bit and used the following pattern under timer->lock to publish cancellation status. lock(t->lock); t->cancelling = true; mb(); if (cur->cancelling) return -EDEADLK; unlock(t->lock); hrtimer_cancel(t->timer); t->cancelling = false; The store outside the critical section could overwrite a parallel requests t->cancelling assignment to true, to ensure the parallely executing callback observes its cancellation status. It would be necessary to clear this cancelling bit once hrtimer_cancel is done, but lack of serialization introduced races. Another option was explored where bpf_timer_start would clear the bit when (re)starting the timer under timer->lock. This would ensure serialized access to the cancelling bit, but may allow it to be cleared before in-flight hrtimer_cancel has finished executing, such that lockups can occur again. Thus, we choose an atomic counter to keep track of all outstanding cancellation requests and use it to prevent lockups in case callbacks attempt to cancel each other while executing in parallel.	5.5	More Details
CVE-2024-42238	In the Linux kernel, the following vulnerability has been resolved: firmware: cs_dsp: Return error if block header overflows file Return an error from cs_dsp_power_up() if a block header is longer than the amount of data left in the file. The previous code in cs_dsp_load() and cs_dsp_load_coeff() would loop while there was enough data left in the file for a valid region. This protected against overrunning the end of the file data, but it didn't abort the file processing with an error.	5.5	More Details
CVE-2024-42237	In the Linux kernel, the following vulnerability has been resolved: firmware: cs_dsp: Validate payload length before processing block Move the payload length check in cs_dsp_load() and cs_dsp_coeff_load() to be done before the block is processed. The check that the length of a block payload does not exceed the number of remaining bytes in the firwmware file buffer was being done near the end of the loop iteration. However, some code before that check used the length field without validating it.	5.5	More Details
CVE-2024-41735	SAP Commerce Backoffice does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability causing low impact on confidentiality and integrity of the application.	5.4	More Details
CVE-2024-7621	The Visual Website Collaboration, Feedback & Project Management – Atarim plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the process_wpfeedback_misc_options() function in all versions up to, and including, 4.0.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update the plugins settings which can also be leveraged to gain access to the plugin's settings.	5.4	More Details
CVE-2024-6134	The wp-cart-for-digital-products WordPress plugin before 8.5.6 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	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7353	The Accept Stripe Payments plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's accept_stripe_payment_ng shortcode in all versions up to, and including, 2.0.86 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.	5.4	More Details
CVE-2024-6136	The wp-cart-for-digital-products WordPress plugin before 8.5.6 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks	5.4	More Details
CVE-2024-40473	A Stored Cross Site Scripting (XSS) vulnerability was found in "manage_houses.php" in SourceCodester Best House Rental Management System v1.0. It allows remote attackers to execute arbitrary code via "House_no" and "Description" parameter fields.	5.4	More Details
CVE-2024-20443	A vulnerability in the web-based management interface of Cisco ISE could allow an authenticated, remote attacker to conduct an XSS attack against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have at least a low-privileged account on an affected device.	5.4	More Details
CVE-2024-33533	An issue was discovered in Zimbra Collaboration (ZCS) 9.0 and 10.0, issue 1 of 2. A reflected cross-site scripting (XSS) vulnerability has been identified in the Zimbra webmail admin interface. This vulnerability occurs due to inadequate input validation of the packages parameter, allowing an authenticated attacker to inject and execute arbitrary JavaScript code within the context of another user's browser session. By uploading a malicious JavaScript file and crafting a URL containing its location in the packages parameter, the attacker can exploit this vulnerability. Subsequently, when another user visits the crafted URL, the malicious JavaScript code is executed.	5.4	More Details
CVE-2024-40478	A Stored Cross Site Scripting (XSS) vulnerability was found in "/admin/afeedback.php" in Kashipara Online Exam System v1.0, which allows remote attackers to execute arbitrary code via "rname" and "email" parameter fields	5.4	More Details
CVE-2024-40481	A Stored Cross Site Scripting (XSS) vulnerability was found in "/admin/view-enquiry.php" in PHPGurukul Old Age Home Management System v1.0, which allows remote attackers to execute arbitrary code via the Contact Us page "message" parameter.	5.4	More Details
CVE-2024-40474	A Reflected Cross Site Scripting (XSS) vulnerability was found in "edit-cate.php" in SourceCodester House Rental Management System v1.0.	5.4	More Details
CVE-2024-6884	The Gutenberg Blocks with AI by Kadence WP WordPress plugin before 3.2.39 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-2024-41613	A Cross Site Scripting (XSS) vulnerability in Symphony CMS 2.7.10 allows remote attackers to inject arbitrary web script or HTML by editing note.	5.4	More Details
CVE-2024-6869	The Falang multilanguage for WordPress plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on several functions in all versions up to, and including, 1.3.52. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update and delete translations and expose the administrator email address.	5.4	More Details
CVE-2024-33536	An issue was discovered in Zimbra Collaboration (ZCS) 9.0 and 10.0. The vulnerability occurs due to inadequate input validation of the res parameter, allowing an authenticated attacker to inject and execute arbitrary JavaScript code within the context of another user's browser session. By uploading a malicious JavaScript file, accessible externally, and crafting a URL containing its location in the res parameter, the attacker can exploit this vulnerability. Subsequently, when another user visits the crafted URL, the malicious JavaScript code is executed.	5.4	More Details
CVE-2024-41243	An Incorrect Access Control vulnerability was found in /smsa/view_marks.php in Kashipara Responsive School Management System v3.2.0, which allows remote unauthenticated attackers to view MARKS details.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42354	Shopware is an open commerce platform. The store-API works with regular entities and not expose all fields for the public API; fields need to be marked as ApiAware in the EntityDefinition. So only ApiAware fields of the EntityDefinition will be encoded to the final JSON. Prior to versions 6.6.5.1 and 6.5.8.13, the processing of the Criteria did not considered ManyToMany associations and so they were not considered properly and the protections didn't get used. This issue cannot be reproduced with the default entities by Shopware, but can be triggered with extensions. Update to Shopware 6.6.5.1 or 6.5.8.13 to receive a patch. For older versions of 6.2, 6.3, and 6.4, corresponding security measures are also available via a plugin.	5.3	More Details
CVE-2024-41250	An Incorrect Access Control vulnerability was found in /smsa/view_students.php in Kashipara Responsive School Management System v3.2.0, which allows remote unauthenticated attackers to view STUDENT details.	5.3	More Details
CVE-2024-42493	Dorsett Controls InfoScan is vulnerable due to a leak of possible sensitive information through the response headers and the rendered JavaScript prior to user login.	5.3	More Details
CVE-2024-42408	The InfoScan client download page can be intercepted with a proxy, to expose filenames located on the system, which could lead to additional information exposure.	5.3	More Details
CVE-2024-39287	Dorsett Controls Central Server update server has potential information leaks with an unprotected file that contains passwords and API keys.	5.3	More Details
CVE-2024-42478	llama.cpp provides LLM inference in C/C++. The unsafe `data` pointer member in the `rpc_tensor` structure can cause arbitrary address reading. This vulnerability is fixed in b3561.	5.3	More Details
CVE-2024-41245	An Incorrect Access Control vulnerability was found in /smsa/view_teachers.php in Kashipara Responsive School Management System v3.2.0, which allows remote unauthenticated attackers to view TEACHER details.	5.3	More Details
CVE-2024-41238	A SQL injection vulnerability in /smsa/student_login.php in Kashipara Responsive School Management System v1.0 allows an attacker to execute arbitrary SQL commands via the "username" parameter.	5.3	More Details
CVE-2024-7741	A vulnerability was found in wanglongcn ltcms 1.0.20 and classified as critical. This issue affects the function downloadFile of the file /api/file/downloadfile of the component API Endpoint. The manipulation of the argument file leads to path traversal. 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.	5.3	More Details
CVE-2024-3958	An issue has been discovered in GitLab CE/EE affecting all versions before 17.0.6, 17.1 prior to 17.1.4, and 17.2 prior to 17.2.2. An issue was found that allows someone to abuse a discrepancy between the Web application display and the git command line interface to social engineer victims into cloning non-trusted code.	5.3	More Details
CVE-2024-41246	An Incorrect Access Control vulnerability was found in /smsa/admin_dashboard.php in Kashipara Responsive School Management System v3.2.0, which allows remote unauthenticated attackers to view administrator dashboard.	5.3	More Details
CVE-2024-6384	"Hot" backup files may be downloaded by underprivileged users, if they are capable of acquiring a unique backup identifier. This issue affects MongoDB Enterprise Server v6.0 versions prior to 6.0.16, MongoDB Enterprise Server v7.0 versions prior to 7.0.11 and MongoDB Enterprise Server v7.3 versions prior to 7.3.3	5.3	More Details
CVE-2024-41432	An IP Spoofing vulnerability has been discovered in Likeshop up to 2.5.7.20210811. This issue allows an attacker to replace their real IP address with any arbitrary IP address, specifically by adding a forged 'X-Forwarded' or 'Client-IP' header to requests. Exploiting IP spoofing, attackers can bypass account lockout mechanisms during attempts to log into admin accounts, spoof IP addresses in requests sent to the server, and impersonate IP addresses that have logged into user accounts, etc.	5.3	More Details
CVE-2024-6552	The Booking for Appointments and Events Calendar – Amelia plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 1.2. 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 Number	Description	Base Score	Reference
CVE-2024-41249	An Incorrect Access Control vulnerability was found in /smsa/view_subject.php in Kashipara Responsive School Management System v3.2.0, which allows remote unauthenticated attackers to view SUBJECT details.	5.3	More Details
CVE-2024-41244	An Incorrect Access Control vulnerability was found in /smsa/view_class.php in Kashipara Responsive School Management System v3.2.0, which allows remote unauthenticated attackers to view CLASS details.	5.3	More Details
CVE-2024-41247	An Incorrect Access Control vulnerability was found in /smsa/add_class.php and /smsa/add_class_submit.php in Kashipara Responsive School Management System v3.2.0, which allows remote unauthenticated attackers to add a new class entry.	5.3	More Details
CVE-2023-20584	IOMMU improperly handles certain special address ranges with invalid device table entries (DTEs), which may allow an attacker with privileges and a compromised Hypervisor to induce DTE faults to bypass RMP checks in SEV-SNP, potentially leading to a loss of guest integrity.	5.3	More Details
CVE-2024-41248	An Incorrect Access Control vulnerability was found in /smsa/add_subject.php and /smsa/add_subject_submit.php in Kashipara Responsive School Management System v3.2.0, which allows remote unauthenticated attackers to add a new subject entry.	5.3	More Details
CVE-2024-42477	llama.cpp provides LLM inference in C/C++. The unsafe `type` member in the `rpc_tensor` structure can cause `global-buffer-overflow`. This vulnerability may lead to memory data leakage. The vulnerability is fixed in b3561.	5.3	More Details
CVE-2024-38760	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in David Maucher Send Users Email allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Send Users Email: from n/a through 1.5.1.	5.3	More Details
CVE-2024-6759	When mounting a remote filesystem using NFS, the kernel did not sanitize remotely provided filenames for the path separator character, "/". This allows readdir(3) and related functions to return filesystem entries with names containing additional path components. The lack of validation described above gives rise to a confused deputy problem. For example, a program copying files from an NFS mount could be tricked into copying from outside the intended source directory, and/or to a location outside the intended destination directory.	5.3	More Details
CVE-2024-41888	Missing Release of Resource after Effective Lifetime vulnerability in Apache Answer. This issue affects Apache Answer: through 1.3.5. The password reset link remains valid within its expiration period even after it has been used. This could potentially lead to the link being misused or hijacked. Users are recommended to upgrade to version 1.3.6, which fixes the issue.	5.3	More Details
CVE-2024-41890	Missing Release of Resource after Effective Lifetime vulnerability in Apache Answer. This issue affects Apache Answer: through 1.3.5. User sends multiple password reset emails, each containing a valid link. Within the link's validity period, this could potentially lead to the link being misused or hijacked. Users are recommended to upgrade to version 1.3.6, which fixes the issue.	5.3	More Details
CVE-2024-41733	In SAP Commerce, valid user accounts can be identified during the customer registration and login processes. This allows a potential attacker to learn if a given e-mail is used for an account, but does not grant access to any customer data beyond this knowledge. The attacker must already know the e-mail that they wish to test for. The impact on confidentiality therefore is low and no impact to integrity or availability	5.3	More Details
CVE-2024-38756	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Weblizar Coming Soon allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Coming Soon: from n/a through 1.6.3.	5.3	More Details
CVE-2024-6562	The affiliate-toolkit – WordPress Affiliate Plugin plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 3.5.5. This is due display_errors being set to true . 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-2024-37930	Exposure of Sensitive Information to an Unauthorized Actor, Missing Authorization vulnerability in ThemeSphere SmartMag allows Excavation, Accessing Functionality Not Properly Constrained by ACLs.This issue affects SmartMag: from n/a through 9.3.0.	5.3	More Details
CVE-2024-37924	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Wp2speed WP2Speed Faster allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects WP2Speed Faster: from n/a through 1.0.1.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7382	The Linkify Text plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 1.9.1. This is due to the plugin utilizing bootstrap and leaving test files with display_errors on. 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-2024-41683	A vulnerability has been identified in Location Intelligence family (All versions < V4.4). Affected products do not properly enforce a strong user password policy. This could facilitate a brute force attack against legitimate user passwords.	5.3	More Details
CVE-2024-7410	The My Custom CSS PHP & ADS plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 3.3. This is due the plugin not preventing direct access to the /my-custom-css/vendor/mobiledetect/mobiledetectlib/export/exportToJSON.php file and and the file displaying/generating the full path. 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-2024-7412	The No Update Nag plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 1.4.12. This is due to the plugin allowing direct access to the bootstrap.php file which has display_errors on. 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-2024-7413	The Obfuscate Email plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 3.8.1. This is due to the plugin allowing direct access to the bootstrap.php file which has display_errors on. 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-2024-7414	The PDF Builder for WPForms plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 1.2.116. This is due to the plugin allowing direct access to the composer-setup.php file which has display_errors on. 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-2024-7416	The Reveal Template plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 3.7. This is due to the plugin allowing direct access to the bootstrap.php file which has display_errors on. 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-2024-7704	A vulnerability was found in Weaver e-cology 8. It has been classified as problematic. Affected is an unknown function of the file /cloudstore/ecode/setup/ecology_dev.zip of the component Source Code Handler. The manipulation leads to information disclosure. 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.	5.3	More Details
CVE-2024-7658	A vulnerability, which was classified as problematic, has been found in projectsend up to r1605. This issue affects the function get_preview of the file process.php. The manipulation leads to improper control of resource identifiers. The attack may be initiated remotely. Upgrading to version r1720 is able to address this issue. The patch is named eb5a04774927e5855b9d0e5870a2aae5a3dc5a08. It is recommended to upgrade the affected component.	5.3	More Details
CVE-2024-41682	A vulnerability has been identified in Location Intelligence family (All versions < V4.4). Affected products do not properly enforce restriction of excessive authentication attempts. This could allow an unauthenticated remote attacker to conduct brute force attacks against legitimate user passwords.	5.3	More Details
CVE-2024-42468	openHAB, a provider of open-source home automation software, has add-ons including the visualization add-on CometVisu. CometVisuServlet in versions prior to 4.2.1 is susceptible to an unauthenticated path traversal vulnerability. Local files on the server can be requested via HTTP GET on the CometVisuServlet. This issue may lead to information disclosure. Users should upgrade to version 4.2.1 of the CometVisu add-on of openHAB to receive a patch.	5.3	More Details
CVE-2024-38749	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Olive Themes Olive One Click Demo Import allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Olive One Click Demo Import: from n/a through 1.1.2.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38742	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in MBE Worldwide S.P.A. MBE eShip allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects MBE eShip: from n/a through 2.1.2.	5.3	More Details
CVE-2023-20509	An insufficient DRAM address validation in PMFW may allow a privileged attacker to perform a DMA read from an invalid DRAM address to SRAM, potentially resulting in loss of data integrity.	5.2	More Details
CVE-2021-46746	Lack of stack protection exploit mechanisms in ASP Secure OS Trusted Execution Environment (TEE) may allow a privileged attacker with access to AMD signing keys to c006Frrupt the return address, causing a stack-based buffer overrun, potentially leading to a denial of service.	5.2	More Details
CVE-2024-34611	Improper access control in KnoxService prior to SMR Aug-2024 Release 1 allows local attackers to get sensitive information.	5.1	More Details
CVE-2024-34610	Improper access control in ExtControlDeviceService prior to SMR Aug-2024 Release 1 allows local attackers to access protected data.	5.1	More Details
CVE-2024-34615	Out-of-bound write in libsmat.so prior to SMR Aug-2024 Release 1 allows local attackers to cause memory corruption.	5.1	More Details
CVE-2024-34616	Improper handling of insufficient permission in KnoxDualDARPolicy prior to SMR Aug-2024 Release 1 allows local attackers to access sensitive data.	5.1	More Details
CVE-2024-36505	An improper access control vulnerability [CWE-284] in FortiOS 7.4.0 through 7.4.3, 7.2.5 through 7.2.7, 7.0.12 through 7.0.14 and 6.4.x may allow an attacker who has already successfully obtained write access to the underlying system (via another hypothetical exploit) to bypass the file integrity checking system.	5.1	More Details
CVE-2023-31310	Improper input validation in Power Management Firmware (PMFW) may allow an attacker with privileges to send a malformed input for the "set temperature input selection" command, potentially resulting in a loss of integrity and/or availability.	5.0	More Details
CVE-2024-41737	SAP CRM ABAP (Insights Management) allows an authenticated attacker to enumerate HTTP endpoints in the internal network by specially crafting HTTP requests. On successful exploitation this can result in information disclosure. It has no impact on integrity and availability of the application.	5.0	More Details
CVE-2024-7554	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.9 before 17.0.6, all versions starting from 17.1 before 17.1.4, all versions starting from 17.2 before 17.2.2. Under certain conditions, access tokens may have been logged when an API request was made in a specific manner.	4.9	More Details
CVE-2024-7355	The Organization chart plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘title_input’ and 'node_description' parameter in all versions up to, and including, 1.5.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. By default, this can only be exploited by administrators, but the ability to use and configure charts can be extended to subscribers.	4.9	More Details
CVE-2024-41614	symphonycms <=2.7.10 is vulnerable to Cross Site Scripting (XSS) in the Comment component for articles.	4.8	More Details
CVE-2024-42367	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.10.2, static routes which contain files with compressed variants (`.gz` or `.br` extension) are vulnerable to path traversal outside the root directory if those variants are symbolic links. The server protects static routes from path traversal outside the root directory when `follow_symlinks=False` (default). It does this by resolving the requested URL to an absolute path and then checking that path relative to the root. However, these checks are not performed when looking for compressed variants in the `FileResponse` class, and symbolic links are then automatically followed when performing the `Path.stat()` and `Path.open()` to send the file. Version 3.10.2 contains a patch for the issue.	4.8	More Details
CVE-2024-6158	The Category Posts Widget WordPress plugin before 4.9.17, term-and-category-based-posts-widget WordPress plugin before 4.9.13 does not validate and escape some of its "Category Posts" widget settings before outputting them back in a page/post where the Widget is embed, 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 Number	Description	Base Score	Reference
CVE-2024-20479	A vulnerability in the web-based management interface of Cisco ISE could allow an authenticated, remote attacker to conduct an XSS attack against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have Admin privileges on an affected device.	4.8	More Details
CVE-2024-6724	The Generate Images WordPress plugin before 5.2.8 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-2024-4350	Concrete CMS versions 9.0.0 to 9.3.2 and below 8.5.18 are vulnerable to Stored XSS in RSS Displayer when user input is stored and later embedded into responses. A rogue administrator could inject malicious code into fields due to insufficient input validation. The Concrete CMS security team gave this vulnerability a CVSS v3.1 score of 3.0 with a vector of AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:N/A:N https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator and a CVSS v4 score of 2.1 with vector CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Thanks, m3dium for reporting.	4.8	More Details
CVE-2024-7394	Concrete CMS versions 9 through 9.3.2 and below 8.5.18 are vulnerable to Stored XSS in getAttributeSetName(). A rogue administrator could inject malicious code. The Concrete CMS team gave this a CVSS v3.1 rank of 2 with vector AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator and a CVSS v4.0 rank of 1.8 with vector CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N . Thanks, m3dium for reporting.	4.8	More Details
CVE-2024-41239	A Stored Cross Site Scripting (XSS) vulnerability was found in "/smsa/add_class_submit.php" in Responsive School Management System v3.2.0, which allows remote attackers to execute arbitrary code via "class_name" parameter field.	4.8	More Details
CVE-2023-31339	Improper input validation in ARM® Trusted Firmware used in AMD's Zynq™ UltraScale+™) MPSoC/RFSoC may allow a privileged attacker to perform out of bound reads, potentially resulting in data leakage and denial of service.	4.8	More Details
CVE-2024-43168	DISPUTE NOTE: this issue does not pose a security risk as it (according to analysis by the original software developer, NLnet Labs) falls within the expected functionality and security controls of the application. Red Hat has made a claim that there is a security risk within Red Hat products. NLnet Labs has no further information about the claim, and suggests that affected Red Hat customers refer to available Red Hat documentation or support channels. ORIGINAL DESCRIPTION: A heap-buffer-overflow flaw was found in the cfg_mark_ports function within Unbound's config_file.c, which can lead to memory corruption. This issue could allow an attacker with local access to provide specially crafted input, potentially causing the application to crash or allowing arbitrary code execution. This could result in a denial of service or unauthorized actions on the system.	4.8	More Details
CVE-2024-41774	IBM Common Licensing 9.0 is vulnerable to stored cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 350348.	4.8	More Details
CVE-2024-6481	The Search & Filter Pro WordPress plugin before 2.5.18 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-2024-7512	Concrete CMS versions 9.0.0 through 9.3.2 are affected by a stored XSS vulnerability in Board instances. A rogue administrator could inject malicious code. The Concrete CMS security team gave this vulnerability a CVSS 4.0 Score of 1.8 with vector: CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N. Versions below 9 are not affected. Thanks, m3dium for reporting.	4.8	More Details
CVE-2024-42482	fish-shop/syntax-check is a GitHub action for syntax checking fish shell files. Improper neutralization of delimiters in the `pattern` input (specifically the command separator `;` and command substitution characters `(` and `)`) mean that arbitrary command injection is possible by modification of the input value used in a workflow. This has the potential for exposure or exfiltration of sensitive information from the workflow runner, such as might be achieved by sending environment variables to an external entity. It is recommended that users update to the patched version `v1.6.12` or the latest release version `v2.0.0`, however remediation may be possible through careful control of workflows and the `pattern` input value used by this action.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41906	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V2.0). The affected application does not properly handle cacheable HTTP responses in the web service. This could allow an attacker to read and modify data stored in the local cache.	4.8	More Details
CVE-2024-7706	A vulnerability was found in Fujian mwcms 1.0.0. It has been rated as critical. Affected by this issue is the function uploadimage of the file /uploadfile.html. The manipulation of the argument upfile leads to unrestricted upload. 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.	4.7	More Details
CVE-2024-42253	In the Linux kernel, the following vulnerability has been resolved: gpio: pca953x: fix pca953x_irq_bus_sync_unlock race Ensure that `i2c_lock' is held when setting interrupt latch and mask in pca953x_irq_bus_sync_unlock() in order to avoid races. The other (non-probe) call site pca953x_gpio_set_multiple() ensures the lock is held before calling pca953x_write_regs(). The problem occurred when a request raced against irq_bus_sync_unlock() approximately once per thousand reboots on an i.MX8MP based system. * Normal case 0-0022: write register All3a {03,02,00,00,01} Input latch P0 0-0022: write register All49 {fc,fd,ff,ff,fe} Interrupt mask P0 0-0022: write register All08 {ff,00,00,00,00} Output P3 0-0022: write register All12 {fc,00,00,00,00} Config P3 * Race case 0-0022: write register All08 {ff,00,00,00,00} Output P3 0-0022: write register All08 {03,02,00,00,01} *** Wrong register *** 0-0022: write register All12 {fc,00,00,00,00} Config P3 0-0022: write register All49 {fc,fd,ff,ff,fe} Interrupt mask P0	4.7	More Details
CVE-2024-41732	SAP NetWeaver Application Server ABAP allows an unauthenticated attacker to craft a URL link that could bypass allowlist controls. Depending on the web applications provided by this server, the attacker might inject CSS code or links into the web application that could allow the attacker to read or modify information. There is no impact on availability of application.	4.7	More Details
CVE-2023-20510	An insufficient DRAM address validation in PMFW may allow a privileged attacker to read from an invalid DRAM address to SRAM, potentially resulting in data corruption or denial of service.	4.7	More Details
CVE-2022-38382	IBM Cloud Pak for Security (CP4S) 1.10.0.0 through 1.10.11.0 and IBM QRadar Suite Software 1.10.12.0 through 1.10.23.0 does not invalidate session after logout which could allow another authenticated user to obtain sensitive information. IBM X-Force ID: 233672.	4.7	More Details
CVE-2024-7705	A vulnerability was found in Fujian mwcms 1.0.0. It has been declared as critical. Affected by this vulnerability is the function uploadeditor of the file /uploadeditor.html?action=uploadimage of the component Image Upload. The manipulation of the argument upfile leads to unrestricted upload. 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.	4.7	More Details
CVE-2024-39922	A vulnerability has been identified in LOGO! 12/24RCE (6ED1052-1MD08-0BA1) (All versions), LOGO! 12/24RCEo (6ED1052-2MD08-0BA1) (All versions), LOGO! 230RCE (6ED1052-1FB08-0BA1) (All versions), LOGO! 230RCEo (6ED1052-2FB08-0BA1) (All versions), LOGO! 24CE (6ED1052-1CC08-0BA1) (All versions), LOGO! 24CEo (6ED1052-2CC08-0BA1) (All versions), LOGO! 24RCE (6ED1052-1HB08-0BA1) (All versions), LOGO! 24RCEo (6ED1052-2HB08-0BA1) (All versions), SIPLUS LOGO! 12/24RCE (6AG1052-1MD08-7BA1) (All versions), SIPLUS LOGO! 12/24RCEo (6AG1052-2MD08-7BA1) (All versions), SIPLUS LOGO! 230RCE (6AG1052-1FB08-7BA1) (All versions), SIPLUS LOGO! 230RCEo (6AG1052-2FB08-7BA1) (All versions), SIPLUS LOGO! 24CE (6AG1052-1CC08-7BA1) (All versions), SIPLUS LOGO! 24CEo (6AG1052-2CC08-7BA1) (All versions), SIPLUS LOGO! 24RCE (6AG1052-1HB08-7BA1) (All versions), SIPLUS LOGO! 24RCEo (6AG1052-2HB08-7BA1) (All versions). Affected devices store user passwords in plaintext without proper protection. This could allow a physical attacker to retrieve them from the embedded storage ICs.	4.6	More Details
CVE-2024-38123	Windows Bluetooth Driver Information Disclosure Vulnerability	4.4	More Details
CVE-2024-42032	Access permission verification vulnerability in the Contacts module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	4.4	More Details
CVE-2024-6691	The Easy Digital Downloads – Sell Digital Files & Subscriptions (eCommerce Store + Payments Made Easy) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the currency value in all versions up to, and including, 3.3.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31356	Incomplete system memory cleanup in SEV firmware could allow a privileged attacker to corrupt guest private memory, potentially resulting in a loss of data integrity.	4.4	More Details
CVE-2024-4207	A cross-site scripting issue has been discovered in GitLab affecting all versions starting from 5.1 prior 17.0.6, starting from 17.1 prior to 17.1.4, and starting from 17.2 prior to 17.2.2. When viewing an XML file in a repository in raw mode, it can be made to render as HTML if viewed under specific circumstances.	4.4	More Details
CVE-2024-7648	The Opal Membership plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.2.4 via the private notes functionality on payments which utilizes WordPress comments. This makes it possible for authenticated attackers, with subscriber-level access and above, to view private notes via recent comments that should be restricted to just administrators.	4.3	More Details
CVE-2024-7645	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file users.php of the component User Page. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2024-22114	User with no permission to any of the Hosts can access and view host count & other statistics through System Information Widget in Global View Dashboard.	4.3	More Details
CVE-2024-7662	A vulnerability was found in SourceCodester Car Driving School Management System 1.0. It has been declared as problematic. This vulnerability affects the function save_package of the file admin/packages/manag_package.php. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2024-7709	A vulnerability, which was classified as problematic, has been found in OcoMon 4.0RC1/4.0/5.0RC1. This issue affects some unknown processing of the file /includes/common/require_access_recovery.php of the component URL Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.0.1 and 5.0 is able to address this issue. It is recommended to upgrade the affected component.	4.3	More Details
CVE-2024-7739	A vulnerability, which was classified as problematic, was found in yzane vscode-markdown-pdf 1.5.0. This affects an unknown part. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2024-42222	In Apache CloudStack 4.19.1.0, a regression in the network listing API allows unauthorised list access of network details for domain admin and normal user accounts. This vulnerability compromises tenant isolation, potentially leading to unauthorised access to network details, configurations and data. Affected users are advised to upgrade to version 4.19.1.1 to address this issue. Users on older versions of CloudStack considering to upgrade, can skip 4.19.1.0 and upgrade directly to 4.19.1.1.	4.3	More Details
CVE-2024-7266	Incorrect User Management vulnerability in Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy EZD RP allows logged-in user to list all users in the system, including those from other organizations. This issue affects EZD RP: from 15 before 15.84, from 16 before 16.15, from 17 before 17.2.	4.3	More Details
CVE-2024-41736	Under certain conditions SAP Permit to Work allows an authenticated attacker to access information which would otherwise be restricted causing low impact on the confidentiality of the application.	4.3	More Details
CVE-2024-7661	A vulnerability was found in SourceCodester Car Driving School Management System 1.0. It has been classified as problematic. This affects the function save_users of the file admin/user/index.php. The manipulation leads to cross-site request forgery. 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-2024-3114	An issue was discovered in GitLab CE/EE affecting all versions starting from 11.10 prior to 17.0.6, 17.1 prior to 17.1.4, and 17.2 prior to 17.2.2, with the processing logic for parsing invalid commits can lead to a regular expression DoS attack on the server.	4.3	More Details
CVE-2024-42375	SAP BusinessObjects Business Intelligence Platform allows an authenticated attacker to upload malicious code over the network, that could be executed by the application. On successful exploitation, the attacker can cause a low impact on the Integrity of the application.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41734	Due to missing authorization check in SAP NetWeaver Application Server ABAP and ABAP Platform, an authenticated attacker could call an underlying transaction, which leads to disclosure of user related information. There is no impact on integrity or availability.	4.3	More Details
CVE-2024-7610	A Denial of Service (DoS) condition has been discovered in GitLab CE/EE affecting all versions starting with 15.9 before 17.0.6, 17.1 prior to 17.1.4, and 17.2 prior to 17.2.2. It is possible for an attacker to cause catastrophic backtracking while parsing results from Elasticsearch.	4.3	More Details
CVE-2024-41941	A vulnerability has been identified in SINEC NMS (All versions < V3.0). The affected application does not properly enforce authorization checks. This could allow an authenticated attacker to bypass the checks and modify settings in the application without authorization.	4.3	More Details
CVE-2024-6824	The Premium Addons for Elementor plugin for WordPress is vulnerable to unauthorized modification and loss of data due to a missing capability check on the 'check_temp_validity' and 'update_template_title' functions in all versions up to, and including, 4.10.38. This makes it possible for authenticated attackers, with Contributor-level access and above, to delete arbitrary content and update post and page titles.	4.3	More Details
CVE-2024-42164	Insufficiently random values for generating password reset token in FIWARE Keyrock <= 8.4 allow attackers to disable two factor authorization of any user by predicting the token for the disable_2fa link.	4.3	More Details
CVE-2024-6987	The Orchid Store theme for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'orchid_store_activate_plugin' function in all versions up to, and including, 1.5.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to activate the Addonify Floating Cart For WooCommerce plugin if it is installed.	4.3	More Details
CVE-2024-42373	SAP Student Life Cycle Management (SLcM) fails to conduct proper authorization checks for authenticated users, leading to the potential escalation of privileges. On successful exploitation it could allow an attacker to delete non-sensitive report variants that are typically restricted, causing minimal impact on the integrity of the application.	4.3	More Details
CVE-2024-42377	SAP shared service framework allows an authenticated non-administrative user to call a remote-enabled function, which will allow them to insert value entries into a non-sensitive table, causing low impact on integrity of the application	4.3	More Details
CVE-2024-39591	SAP Document Builder does not perform necessary authorization checks for one of the function modules resulting in escalation of privileges causing low impact on confidentiality of the application.	4.3	More Details
CVE-2024-6254	The Brizy – Page Builder plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.5.1. This is due to missing or incorrect nonce validation on form submissions. This makes it possible for unauthenticated attackers to submit forms intended for public use as another user via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. On sites where unfiltered_html is enabled, this can lead to the admin unknowingly adding a Stored Cross-Site Scripting payload.	4.3	More Details
CVE-2024-4784	An issue was discovered in GitLab EE starting from version 16.7 before 17.0.6, version 17.1 before 17.1.4 and 17.2 before 17.2.2 that allowed bypassing the password re-entry requirement to approve a policy.	4.2	More Details
CVE-2024-7480	An Improper access control vulnerability was found in Avaya Aura System Manager which could allow a command-line interface (CLI) user with administrative privileges to read arbitrary files on the system. Affected versions include 10.1.x.x and 10.2.x.x. Versions prior to 10.1 are end of manufacturer support.	4.2	More Details
CVE-2024-32765	A vulnerability has been reported to affect Network & Virtual Switch. If exploited, the vulnerability could allow local authenticated administrators to gain access to and execute certain functions via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later	4.2	More Details
CVE-2024-0104	NVIDIA Mellanox OS, ONYX, Skyway, MetroX-2 and MetroX-3 XC contain a vulnerability in the LDAP AAA component, where a user can cause improper access. A successful exploit of this vulnerability might lead to information disclosure, data tampering, and escalation of privileges.	4.2	More Details
CVE-2024-41907	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V2.0). The affected application is missing general HTTP security headers in the web server. This could allow an attacker to make the servers more prone to clickjacking attack.	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38143	Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability	4.2	More Details
CVE-2024-34634	Out-of-bounds read in parsing connected object list in Samsung Notes prior to version 4.4.21.62 allows local attacker to access unauthorized memory.	4.0	More Details
CVE-2024-34635	Out-of-bounds read in parsing textbox object in Samsung Notes prior to version 4.4.21.62 allows local attacker to access unauthorized memory.	4.0	More Details
CVE-2024-7388	The WP Bannerize Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via banner alt data in all versions up to, and including, 1.9.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with editor-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.	4.0	More Details
CVE-2024-34632	Out-of-bounds read in uuid parsing in Samsung Notes prior to version 4.4.21.62 allows local attacker to access unauthorized memory.	4.0	More Details
CVE-2024-34633	Out-of-bounds read in parsing object header in Samsung Notes prior to version 4.4.21.62 allows local attacker to access unauthorized memory.	4.0	More Details
CVE-2024-34617	Improper handling of insufficient permission in Telephony prior to SMR Aug-2024 Release 1 allows local attackers to configure default Message application.	4.0	More Details
CVE-2023-7265	Permission verification vulnerability in the lock screen module Impact: Successful exploitation of this vulnerability may affect availability	4.0	More Details
CVE-2024-34618	Improper access control in System property prior to SMR Aug-2024 Release 1 allows local attackers to access cell related information.	4.0	More Details
CVE-2024-34613	Improper access control in Galaxy Watch prior to SMR Aug-2024 Release 1 allows local attackers to access sensitive information of Galaxy watch.	4.0	More Details
CVE-2024-34636	Use of implicit intent for sensitive communication in Samsung Email prior to version 6.1.94.2 allows local attackers to get sensitive information.	4.0	More Details
CVE-2021-46772	Insufficient input validation in the ABL may allow a privileged attacker with access to the BIOS menu or UEFI shell to tamper with the structure headers in SPI ROM causing an out of bounds memory read and write, potentially resulting in memory corruption or denial of service.	3.9	More Details
CVE-2021-26387	Insufficient access controls in ASP kernel may allow a privileged attacker with access to AMD signing keys and the BIOS menu or UEFI shell to map DRAM regions in protected areas, potentially leading to a loss of platform integrity.	3.9	More Details
CVE-2024-5445	Ecosystem Agent version 4 < 4.5.1.2597 and Ecosystem Agent version 5 < 5.1.4.2473 did not properly validate SSL/TLS certificates, which could allow a malicious actor to perform a Man-in-the-Middle and intercept traffic between the agent and N-able servers from a privileged network position.	3.8	More Details
CVE-2022-45862	An insufficient session expiration vulnerability [CWE-613] vulnerability in FortiOS 7.2.5 and below, 7.0 all versions, 6.4 all versions; FortiProxy 7.2 all versions, 7.0 all versions; FortiPAM 1.3 all versions, 1.2 all versions, 1.1 all versions, 1.0 all versions; FortiSwitchManager 7.2.1 and below, 7.0 all versions GUI may allow attackers to re-use websessions after GUI logout, should they manage to acquire the required credentials.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7659	A vulnerability, which was classified as problematic, was found in projectsend up to r1605. Affected is the function generate_random_string of the file includes/functions.php of the component Password Reset Token Handler. The manipulation leads to insufficiently random values. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. Upgrading to version r1720 is able to address this issue. The name of the patch is aa27eb97edc2ff2b203f97e6675d7b5ba0a22a17. It is recommended to upgrade the affected component.	3.7	More Details
CVE-2024-28166	SAP BusinessObjects Business Intelligence Platform allows an authenticated attacker to upload malicious code over the network, that could be executed by the application. On successful exploitation, the attacker can cause a low impact on the Integrity of the application.	3.7	More Details
CVE-2024-7644	A vulnerability was found in SourceCodester Leads Manager Tool 1.0. It has been classified as problematic. This affects an unknown part of the file /endpoint/add-leads.php of the component Add Leads Handler. The manipulation of the argument leads_name/phone_number 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.	3.5	More Details
CVE-2024-7733	A vulnerability, which was classified as problematic, was found in FastCMS up to 0.1.5. Affected is an unknown function of the component New Article Category Page. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-7657	A vulnerability classified as problematic was found in Gila CMS 1.10.9. This vulnerability affects unknown code of the file /cm/update_rows/page?id=2 of the component HTTP POST Request Handler. The manipulation of the argument content leads to cross site scripting. 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.	3.5	More Details
CVE-2024-7660	A vulnerability has been found in SourceCodester File Manager App 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Add File Handler. The manipulation of the argument File Title/Uploaded By leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-7677	A vulnerability was found in SourceCodester Car Driving School Management System 1.0. It has been declared as problematic. Affected by this vulnerability is the function update_settings_info of the file /classes/SystemSettings.php?f=update_settings. The manipulation of the argument contact/address leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-7749	A vulnerability, which was classified as problematic, was found in SourceCodester Accounts Manager App 1.0. Affected is an unknown function of the file /endpoint/add-account.php. The manipulation of the argument account_name leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-7686	A vulnerability, which was classified as problematic, was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. This affects an unknown part of the file register_case.php. The manipulation of the argument title/description/opposite_lawyer 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.	3.5	More Details
CVE-2024-7685	A vulnerability, which was classified as problematic, has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0. Affected by this issue is some unknown functionality of the file adds.php. The manipulation of the argument name/dob/email/mobile/address 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-2024-7684	A vulnerability classified as problematic was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. Affected by this vulnerability is an unknown functionality of the file add_act.php. The manipulation of the argument aname leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-7683	A vulnerability classified as problematic has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0. Affected is an unknown function of the file addcase_stage.php. The manipulation of the argument cname leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-7678	A vulnerability was found in SourceCodester Car Driving School Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /classes/Master.php?f=save_package. The manipulation of the argument name/description/training_duration 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-2024-0102	NVIDIA CUDA Toolkit for all platforms contains a vulnerability in nvdisasm, where an attacker can cause an out-of-bounds read issue by deceiving a user into reading a malformed ELF file. A successful exploit of this vulnerability might lead to denial of service.	3.3	More Details
CVE-2024-6692	The Easy Digital Downloads – Sell Digital Files & Subscriptions (eCommerce Store + Payments Made Easy) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Agreement Text value in all versions up to, and including, 3.3.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	3.3	More Details
CVE-2024-42249	In the Linux kernel, the following vulnerability has been resolved: spi: don't unoptimize message in spi_async() Calling spi_maybe_unoptimize_message() in spi_async() is wrong because the message is likely to be in the queue and not transferred yet. This can corrupt the message while it is being used by the controller driver. spi_maybe_unoptimize_message() is already called in the correct place in spi_finalize_current_message() to balance the call to spi_maybe_optimize_message() in spi_async().	3.3	More Details
CVE-2024-42233	In the Linux kernel, the following vulnerability has been resolved: filemap: replace pte_offset_map() with pte_offset_map_nolock() The vmf->ptl in filemap_fault_recheck_pte_none() is still set from handle_pte_fault(). But at the same time, we did a pte_unmap(vmf->pte). After a pte_unmap(vmf->pte) unmap and rcu_read_unlock(), the page table may be racily changed and vmf->ptl maybe fails to protect the actual page table. Fix this by replacing pte_offset_map() with pte_offset_map_nolock(). As David said, the PTL pointer might be stale so if we continue to use it infilemap_fault_recheck_pte_none(), it might trigger UAF. Also, if the PTL fails, the issue fixed by commit 58f327f2ce80 ("filemap: avoid unnecessary major faults in filemap_fault()") might reappear.	3.3	More Details
CVE-2023-31366	Improper input validation in AMD µProf could allow an attacker to perform a write to an invalid address, potentially resulting in denial of service.	3.3	More Details
CVE-2023-20513	An insufficient bounds check in PMFW (Power Management Firmware) may allow an attacker to utilize a malicious VF (virtualization function) to send a malformed message, potentially resulting in a denial of service.	3.3	More Details
CVE-2024-7738	A vulnerability, which was classified as problematic, has been found in yzane vscode-markdown-pdf 1.5.0. Affected by this issue is some unknown functionality of the component Markdown File Handler. The manipulation leads to pathname traversal. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used.	3.3	More Details
CVE-2024-41731	SAP BusinessObjects Business Intelligence Platform allows an authenticated attacker to upload malicious code over the network, that could be executed by the application. On successful exploitation, the attacker can cause a low impact on the Integrity of the application.	3.1	More Details
CVE-2024-22122	Zabbix allows to configure SMS notifications. AT command injection occurs on "Zabbix Server" because there is no validation of "Number" field on Web nor on Zabbix server side. Attacker can run test of SMS providing specially crafted phone number and execute additional AT commands on modem.	3.0	More Details
CVE-2024-43167	DISPUTE NOTE: this issue does not pose a security risk as it (according to analysis by the original software developer, NLnet Labs) falls within the expected functionality and security controls of the application. Red Hat has made a claim that there is a security risk within Red Hat products. NLnet Labs has no further information about the claim, and suggests that affected Red Hat customers refer to available Red Hat documentation or support channels. ORIGINAL DESCRIPTION: A NULL pointer dereference flaw was found in the ub_ctx_set_fwd function in Unbound. This issue could allow an attacker who can invoke specific sequences of API calls to cause a segmentation fault. When certain API functions such as ub_ctx_set_fwd and ub_ctx_resolvconf are called in a particular order, the program attempts to read from a NULL pointer, leading to a crash. This issue can result in a denial of service by causing the application to terminate unexpectedly.	2.8	More Details
CVE-2024-22123	Setting SMS media allows to set GSM modem file. Later this file is used as Linux device. But due everything is a file for Linux, it is possible to set another file, e.g. log file and zabbix_server will try to communicate with it as modem. As a result, log file will be broken with AT commands and small part for log file content will be leaked to UI.	2.7	More Details
CVE-2024-42036	Access permission verification vulnerability in the Notepad module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2.5	More Details
CVE-2023-31304	Improper input validation in SMU may allow an attacker with privileges and a compromised physical function (PF) to modify the PCIe® lane count and speed, potentially leading to a loss of availability.	2.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31307	Improper validation of array index in Power Management Firmware (PMFW) may allow a privileged attacker to cause an out-of-bounds memory read within PMFW, potentially leading to a denial of service.	2.3	More Details
CVE-2023-20512	A hardcoded AES key in PMFW may result in a privileged attacker gaining access to the key, potentially resulting in internal debug information leakage.	1.9	More Details
CVE-2023-20518	Incomplete cleanup in the ASP may expose the Master Encryption Key (MEK) to a privileged attacker with access to the BIOS menu or UEFI shell and a memory exfiltration vulnerability, potentially resulting in loss of confidentiality.	1.9	More Details
CVE-2023-31305	Generation of weak and predictable Initialization Vector (IV) in PMFW (Power Management Firmware) may allow an attacker with privileges to reuse IV values to reverse-engineer debug data, potentially resulting in information disclosure.	1.9	More Details
CVE-2024-43359	ZoneMinder is a free, open source closed-circuit television software application. ZoneMinder has a cross-site scripting vulnerability in the montagereview via the displayinterval, speed, and scale parameters. This vulnerability is fixed in 1.36.34 and 1.37.61.	0.0	More Details
CVE-2024-6768	A Denial of Service in CLFS.sys in Microsoft Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, and Windows Server 2022 allows a malicious authenticated low-privilege user to cause a Blue Screen of Death via a forced call to the KeBugCheckEx function.	N/A	More Details
CVE-2024-2259	This vulnerability exists in InstaRISPACS software due to insufficient validation of user supplied input for the loginTo parameter in user login module of the web interface of the application. A remote attacker could exploit this vulnerability by sending a specially crafted input to the vulnerable parameter to perform reflected Cross Site Scripting (XSS) attacks on the targeted system.	N/A	More Details
CVE-2024-38688	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-7113	If exploited, this vulnerability could cause a SuiteLink server to consume excessive system resources and slow down processing of Data I/O for the duration of the attack.	N/A	More Details
CVE-2024-6619	In Ocean Data Systems Dream Report, an incorrect permission vulnerability could allow a local unprivileged attacker to escalate their privileges and could cause a denial-of-service.	N/A	More Details
CVE-2024-6618	In Ocean Data Systems Dream Report, a path traversal vulnerability could allow an attacker to perform remote code execution through the injection of a malicious dynamic-link library (DLL).	N/A	More Details
CVE-2024-5800	Diffie-Hellman groups with insufficient strength are used in the SSL/TLS stack of B&R Automation Runtime versions before 6.0.2, allowing a network attacker to decrypt the SSL/TLS communication.	N/A	More Details
CVE-2024-5801	Enabled IP Forwarding feature in B&R Automation Runtime versions before 6.0.2 may allow remote attack-ers to compromise network security by routing IP-based packets through the host, potentially by-passing firewall, router, or NAC filtering.	N/A	More Details
CVE-2024-37283	An issue was discovered whereby Elastic Agent will leak secrets from the agent policy elastic-agent.yml only when the log level is configured to debug. By default the log level is set to info, where no leak occurs.	N/A	More Details
CVE-2024-6684	Authentication Bypass Using an Alternate Path or Channel vulnerability in GST Electronics inohom Nova Panel N7 allows Authentication Bypass.This issue affects inohom Nova Panel N7: through 1.9.9.6. NOTE: The vendor was contacted and it was learned that the product is not supported.	N/A	More Details
CVE-2022-38322	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7123	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-21881	Inadequate Encryption Strength vulnerability allow an authenticated attacker to execute arbitrary OS Commands via encrypted package upload.This issue affects Envoy: 4.x and 5.x	N/A	More Details
CVE-2024-7633	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2024-7567	A denial-of-service vulnerability exists via the CIP/Modbus port in the Rockwell Automation Micro850/870 (2080 -L50E/2080 -L70E). If exploited, the CIP/Modbus communication may be disrupted for short duration.	N/A	More Details
CVE-2024-6079	A vulnerability exists in the Rockwell Automation Emulate3D™, which could be leveraged to execute a DLL Hijacking attack. The application loads shared libraries, which are readable and writable by any user. If exploited, a malicious user could leverage a malicious dll and perform a remote code execution attack.	N/A	More Details
CVE-2024-3973	The House Manager WordPress plugin through 1.0.8.4 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	N/A	More Details
CVE-2024-3279	An improper access control vulnerability exists in the mintplex-labs/anything-llm application, specifically within the import endpoint. This vulnerability allows an anonymous attacker, without an account in the application, to import their own database file, leading to the deletion or spoofing of the existing `anythingllm.db` file. By exploiting this vulnerability, attackers can serve malicious data to users or collect information about them. The vulnerability stems from the application's failure to properly restrict access to the data-import functionality, allowing unauthorized database manipulation.	N/A	More Details
CVE-2024-7121	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details