SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 13 November 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-2024-51790	Unrestricted Upload of File with Dangerous Type vulnerability in Team HB WEBSOL HB AUDIO GALLERY allows Upload a Web Shell to a Web Server.This issue affects HB AUDIO GALLERY: from n/a through 3.0.	10.0	More Details
CVE-2024-51788	Unrestricted Upload of File with Dangerous Type vulnerability in Joshua Wolfe The Novel Design Store Directory allows Upload a Web Shell to a Web Server.This issue affects The Novel Design Store Directory: from n/a through 4.3.0.	10.0	More Details
CVE-2024-8615	The JobSearch WP Job Board plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the jobsearch_location_load_excel_file_callback() function in all versions up to, and including, 2.6.7. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	10.0	More Details
CVE-2024-10081	CodeChecker is an analyzer tooling, defect database and viewer extension for the Clang Static Analyzer and Clang Tidy. Authentication bypass occurs when the API URL ends with Authentication. This bypass allows superuser access to all API endpoints other than Authentication. These endpoints include the ability to add, edit, and remove products, among others. All endpoints, apart from the /Authentication is affected by the vulnerability. This issue affects CodeChecker: through 6.24.1.	10.0	More Details
CVE-2024-20418	A vulnerability in the web-based management interface of Cisco Unified Industrial Wireless Software for Cisco Ultra-Reliable Wireless Backhaul (URWB) Access Points could allow an unauthenticated, remote attacker to perform command injection attacks with root privileges on the underlying operating system. This vulnerability is due to improper validation of input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system of the affected device.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44102	A vulnerability has been identified in PP TeleControl Server Basic 1000 to 5000 V3.1 (6NH9910-0AA31-0AE1) (All versions < V3.1.2.1 with redundancy configured), PP TeleControl Server Basic 256 to 1000 V3.1 (6NH9910-0AA31-0AD1) (All versions < V3.1.2.1 with redundancy configured), PP TeleControl Server Basic 32 to 64 V3.1 (6NH9910-0AA31-0AF1) (All versions < V3.1.2.1 with redundancy configured), PP TeleControl Server Basic 64 to 256 V3.1 (6NH9910-0AA31-0AC1) (All versions < V3.1.2.1 with redundancy configured), PP TeleControl Server Basic 8 to 32 V3.1 (6NH9910-0AA31-0AB1) (All versions < V3.1.2.1 with redundancy configured), TeleControl Server Basic 1000 V3.1 (6NH9910-0AA31-0AD0) (All versions < V3.1.2.1 with redundancy configured), TeleControl Server Basic 256 V3.1 (6NH9910-0AA31-0AC0) (All versions < V3.1.2.1 with redundancy configured), TeleControl Server Basic 32 V3.1 (6NH9910-0AA31-0AF0) (All versions < V3.1.2.1 with redundancy configured), TeleControl Server Basic 5000 V3.1 (6NH9910-0AA31-0AE0) (All versions < V3.1.2.1 with redundancy configured), TeleControl Server Basic 64 V3.1 (6NH9910-0AA31-0AB0) (All versions < V3.1.2.1 with redundancy configured), TeleControl Server Basic 8 V3.1 (6NH9910-0AA31-0AA0) (All versions < V3.1.2.1 with redundancy configured), TeleControl Server Basic Serv Upgr (6NH9910-0AA31-0GA1) (All versions < V3.1.2.1 with redundancy configured), TeleControl Server Basic Upgr V3.1 (6NH9910-0AA31-0GA0) (All versions < V3.1.2.1 with redundancy configured). The affected system allows remote users to send maliciously crafted objects. Due to insecure deserialization of user-supplied content by the affected software, an unauthenticated attacker could exploit this vulnerability by sending a maliciously crafted serialized object. This could allow the attacker to execute arbitrary code on the device with SYSTEM privileges.	10.0	More Details
CVE-2024-51793	Unrestricted Upload of File with Dangerous Type vulnerability in Webful Creations Computer Repair Shop allows Upload a Web Shell to a Web Server.This issue affects Computer Repair Shop: from n/a through 3.8115.	10.0	More Details
CVE-2024-51792	Unrestricted Upload of File with Dangerous Type vulnerability in Dang Ngoc Binh Audio Record allows Upload a Web Shell to a Web Server.This issue affects Audio Record: from n/a through 1.0.	10.0	More Details
CVE-2024-51791	Unrestricted Upload of File with Dangerous Type vulnerability in Made I.T. Forms allows Upload a Web Shell to a Web Server.This issue affects Forms: from n/a through 2.8.0.	10.0	More Details
CVE-2024-51789	Unrestricted Upload of File with Dangerous Type vulnerability in UjW0L Image Classify allows Upload a Web Shell to a Web Server.This issue affects Image Classify: from n/a through 1.0.0.	10.0	More Details
CVE-2024-43602	Azure CycleCloud Remote Code Execution Vulnerability	9.9	More Details
CVE-2024-46888	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 3). The affected application does not properly sanitize user provided paths for SFTP-based file up- and downloads. This could allow an authenticated remote attacker to manipulate arbitrary files on the filesystem and achieve arbitrary code execution on the device.	9.9	More Details
CVE-2024-8614	The JobSearch WP Job Board plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the jobsearch_wp_handle_upload() function in all versions up to, and including, 2.6.7. This makes it possible for authenticated attackers, with subscriber-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.9	More Details
CVE-2024-9307	The mFolio Lite plugin for WordPress is vulnerable to file uploads due to a missing capability check in all versions up to, and including, 1.2.1. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file or upload arbitrary EXE files on the affected site's server which may make remote code execution possible if the attacker can also gain access to run the .exe file, or trick a site visitor into downloading and running the .exe file.	9.9	More Details
CVE-2024-11068	The D-Link DSL6740C modem has an Incorrect Use of Privileged APIs vulnerability, allowing unauthenticated remote attackers to modify any user’s password by leveraging the API, thereby granting access to Web, SSH, and Telnet services using that user’s account.	9.8	More Details
CVE-2024-25254	SuperScan v4.1 was discovered to contain a buffer overflow via the Hostname/IP parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50766	SourceCodester Survey Application System 1.0 is vulnerable to SQL Injection in takeSurvey.php via the id parameter.	9.8	More Details
CVE-2024-11016	Webopac from Grand Vice info has a SQL Injection vulnerability, allowing unauthenticated remote attacks to inject arbitrary SQL commands to read, modify, and delete database contents.	9.8	More Details
CVE-2024-11018	Webopac from Grand Vice info does not properly validate uploaded file types, allowing unauthenticated remote attackers to upload and execute webshells, which could lead to arbitrary code execution on the server.	9.8	More Details
CVE-2024-11020	Webopac from Grand Vice info has a SQL Injection vulnerability, allowing unauthenticated remote attacks to inject arbitrary SQL commands to read, modify, and delete database contents.	9.8	More Details
CVE-2024-50989	A SQL injection vulnerability in /omrs/admin/search.php in PHPGurukul Online Marriage Registration System v1.0 allows an attacker to execute arbitrary SQL commands via the "searchdata " parameter.	9.8	More Details
CVE-2024-50667	The boa httpd of Trendnet TEW-820AP 1.01.B01 has a stack overflow vulnerability in /boafrm/formIPv6Addr, /boafrm/formIpv6Setup, /boafrm/formDnsv6. The reason is that the check of ipv6 address is not sufficient, which allows attackers to construct payloads for attacks.	9.8	More Details
CVE-2024-51135	An XML External Entity (XXE) vulnerability in the component DocumentBuilderFactory of powertac-server v1.9.0 allows attackers to access sensitive information or execute arbitrary code via supplying a crafted request containing malicious XML entities.	9.8	More Details
CVE-2024-36061	EnGenius EWS356-FIT devices through 1.1.30 allow blind OS command injection. This allows an attacker to execute arbitrary OS commands via shell metacharacters to the Ping and Speed Test utilities.	9.8	More Details
CVE-2024-44546	Powerjob >= 3.20 is vulnerable to SQL injection via the version parameter.	9.8	More Details
CVE-2024-25255	Sublime Text 4 was discovered to contain a command injection vulnerability via the New Build System module. NOTE: multiple third parties report that this is intended behavior.	9.8	More Details
CVE-2023-27195	Trimble TM4Web 22.2.0 allows unauthenticated attackers to access /inc/tm_ajax.msw?func=UserfromUUID&uuid= to retrieve the last registration access code and use this access code to register a valid account. via a PUT /inc/tm_ajax.msw request. If the access code was used to create an Administrator account, attackers are also able to register new Administrator accounts with full privileges.	9.8	More Details
CVE-2024-50636	PyMOL 2.5.0 contains a vulnerability in its "Run Script" function, which allows the execution of arbitrary Python code embedded within .PYM files. Attackers can craft a malicious .PYM file containing a Python reverse shell payload and exploit the function to achieve Remote Command Execution (RCE). This vulnerability arises because PyMOL treats .PYM files as Python scripts without properly validating or restricting the commands within the script, enabling attackers to run unauthorized commands in the context of the user running the application.	9.8	More Details
CVE-2024-52533	gio/gsocks4aproxy.c in GNOME GLib before 2.82.1 has an off-by-one error and resultant buffer overflow because SOCKS4_CONN_MSG_LEN is not sufficient for a trailing '\0' character.	9.8	More Details
CVE-2024-10245	The Relais 2FA plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 1.0. This is due to incorrect authentication and capability checking in the 'rl_do_ajax' 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 email.	9.8	More Details
CVE-2019-20461	An issue was discovered on Alecto IVM-100 2019-11-12 devices. The device uses a custom UDP protocol to start and control video and audio services. The protocol has been partially reverse engineered. Based upon the reverse engineering, no password or username is ever transferred over this protocol. Thus, one can set up the camera connection feed with only the encoded UID. It is possible to set up sessions with the camera over the Internet by using the encoded UID and the custom UDP protocol, because authentication happens at the client side.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50330	SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote unauthenticated attacker to achieve remote code execution.	9.8	More Details
CVE-2024-52297	Tolgee is an open-source localization platform. Tolgee 3.81.1 included the all configuration properties in the PublicConfiguratioDTO publicly exposed to users. This vulnerability is fixed in v3.81.2.	9.8	More Details
CVE-2024-49369	Icinga is a monitoring system which checks the availability of network resources, notifies users of outages, and generates performance data for reporting. The TLS certificate validation in all Icinga 2 versions starting from 2.4.0 was flawed, allowing an attacker to impersonate both trusted cluster nodes as well as any API users that use TLS client certificates for authentication (ApiUser objects with the client_cn attribute set). This vulnerability has been fixed in v2.14.3, v2.13.10, v2.12.11, and v2.11.12.	9.8	More Details
CVE-2024-43498	.NET and Visual Studio Remote Code Execution Vulnerability	9.8	More Details
CVE-2024-43639	Windows KDC Proxy Remote Code Execution Vulnerability	9.8	More Details
CVE-2020-8007	The pwrstudio web application of EV Charger (in the server in Circontrol Raption through 5.6.2) is vulnerable to OS command injection via three fields of the configuration menu for ntpserver0, ntpserver1, and pingip.	9.8	More Details
CVE-2024-28729	An issue in DLink DWR 2000M 5G CPE With Wifi 6 Ax1800 and Dlink DWR 5G CPE DWR-2000M_1.34ME allows a local attacker to execute arbitrary code via a crafted request.	9.8	More Details
CVE-2024-10586	The Debug Tool plugin for WordPress is vulnerable to arbitrary file creation due to a missing capability check on the dbt_pull_image() function and missing file type validation in all versions up to, and including, 2.2. This makes it possible for unauthenticated attackers to to create arbitrary files such as .php files that can be leveraged for remote code execution.	9.8	More Details
CVE-2024-10625	The WooCommerce Support Ticket System plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the delete_tmp_uploaded_file() function in all versions up to, and including, 17.7. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	9.8	More Details
CVE-2024-51211	SQL injection vulnerability exists in OS4ED openSIS-Classic Version 9.1, specifically in the resetuserinfo.php file. The vulnerability is due to improper input validation of the $username_stn_id parameter, which can be manipulated by an attacker to inject arbitrary SQL commands.	9.8	More Details
CVE-2024-48073	sunniwell HT3300 before 1.0.0.B022.2 is vulnerable to Insecure Permissions. The /usr/local/bin/update program, which is responsible for updating the software in the HT3300 device, is given the execution mode of sudo NOPASSWD. This program is vulnerable to a command injection vulnerability, which could allow an attacker to pass commands to this program via command line arguments to gain elevated root privileges.	9.8	More Details
CVE-2024-46613	WeeChat before 4.4.2 has an integer overflow and resultant buffer overflow at core/core-string.c when there are more than two billion items in a list. This affects string_free_split_shared , string_free_split, string_free_split_command, and string_free_split_tags.	9.8	More Details
CVE-2024-35426	vmir e8117 was discovered to contain a stack overflow via the init_local_vars function at /src/vmir_wasm_parser.c.	9.8	More Details
CVE-2024-10871	The Category Ajax Filter plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.8.2 via the 'params[caf-post-layout]' parameter. This makes it possible for unauthenticated attackers to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where files with a .php extension can be uploaded and included.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10801	The WordPress User Extra Fields plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the ajax_manage_file_chunk_upload() function in all versions up to, and including, 16.5. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. User registration must be enabled for this to be exploited.	9.8	More Details
CVE-2024-10589	The Leopard - WordPress Offload Media plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the import_settings() function in all versions up to, and including, 3.1.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update arbitrary options on the WordPress site. This can be leveraged to update the default role for registration to administrator and enable user registration for attackers to gain administrative user access to a vulnerable site.	9.8	More Details
CVE-2024-10547	The WP Membership plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the user_profile_image_upload() function in all versions up to, and including, 1.6.2. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2024-10284	The CE21 Suite plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.2.0. This is due to hardcoded encryption key in the 'ce21_authentication_phrase' 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 email.	9.8	More Details
CVE-2024-10285	The CE21 Suite plugin for WordPress is vulnerable to sensitive information disclosure via the plugin-log.txt in versions up to, and including, 2.2.0. This makes it possible for unauthenticated attackers to log in the user associated with the JWT token.	9.8	More Details
CVE-2024-10508	The RegistrationMagic – User Registration Plugin with Custom Registration Forms plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 6.0.2.6. This is due to the plugin not properly validating the password reset token prior to updating a user's password. This makes it possible for unauthenticated attackers to reset the password of arbitrary users, including administrators, and gain access to these accounts.	9.8	More Details
CVE-2024-50588	An unauthenticated attacker with access to the local network of the medical office can use known default credentials to gain remote DBA access to the Elefant Firebird database. The data in the database includes patient data and login credentials among other sensitive data. In addition, this enables an attacker to create and overwrite arbitrary files on the server filesystem with the rights of the Firebird database ("NT AUTHORITY\SYSTEM").	9.8	More Details
CVE-2024-10470	The WPLMS Learning Management System for WordPress, WordPress LMS theme for WordPress is vulnerable to arbitrary file read and deletion due to insufficient file path validation and permissions checks in the readfile and unlink functions in all versions up to, and including, 4.962. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). The theme is vulnerable even when it is not activated.	9.8	More Details
CVE-2024-10627	The WooCommerce Support Ticket System plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the ajax_manage_file_chunk_upload() function in all versions up to, and including, 17.7. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2024-7982	The Registrations for the Events Calendar WordPress plugin before 2.12.4 does not sanitise and escape some parameters when accepting event registrations, which could allow unauthenticated users to perform Cross-Site Scripting attacks.	9.6	More Details
CVE-2024-50966	dingfanzu CMS V1.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/doAdminAction.php?act=addAdmin.	9.3	More Details
CVE-2024-46962	The SYQ com.downloader.video.fast (aka Master Video Downloader) application through 2.0 for Android allows an attacker to execute arbitrary JavaScript code via the com.downloader.video.fast.SpeedMainAct component.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51748	Kanboard is project management software that focuses on the Kanban methodology. An authenticated Kanboard admin can run arbitrary php code on the server in combination with a file write possibility. The user interface language is determined and loaded by the setting `application_language` in the `settings` table. Thus, an attacker who can upload a modified sqlite.db through the dedicated feature, has control over the filepath, which is loaded. Exploiting this vulnerability has one constraint: the attacker must be able to place a file (called translations.php) on the system. However, this is not impossible, think of anonymous FTP server or another application that allows uploading files. Once the attacker has placed its file with the actual php code as the payload, the attacker can craft a sqlite db settings, which uses path traversal to point to the directory, where the `translations.php` file is stored. Then gaining code execution after importing the crafted sqlite.db. This issue has been addressed in version 1.2.42 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	9.1	More Details
CVE-2023-52268	The End-User Portal module before 1.0.65 for FreeScout sometimes allows an attacker to authenticate as an arbitrary user because a session token can be sent to the /auth endpoint. NOTE: this module is not part of freescout-helpdesk/freescout on GitHub.	9.1	More Details
CVE-2024-45763	Dell Enterprise SONiC OS, version(s) 4.1.x, 4.2.x, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution. This is a critical severity vulnerability so Dell recommends customers to upgrade at the earliest opportunity.	9.1	More Details
CVE-2024-51504	When using IPAuthenticationProvider in ZooKeeper Admin Server there is a possibility of Authentication Bypass by Spoofing -- this only impacts IP based authentication implemented in ZooKeeper Admin Server. Default configuration of client's IP address detection in IPAuthenticationProvider, which uses HTTP request headers, is weak and allows an attacker to bypass authentication via spoofing client's IP address in request headers. Default configuration honors X-Forwarded-For HTTP header to read client's IP address. X-Forwarded-For request header is mainly used by proxy servers to identify the client and can be easily spoofed by an attacker pretending that the request comes from a different IP address. Admin Server commands, such as snapshot and restore arbitrarily can be executed on successful exploitation which could potentially lead to information leakage or service availability issues. Users are recommended to upgrade to version 3.9.3, which fixes this issue.	9.1	More Details
CVE-2024-50811	hopetree izone lts c011b48 contains a server-side request forgery (SSRF) vulnerability in the active push function as \\apps\\tool\\apis\\bd_push.py does not securely filter user input through push_urls() and get_urls().	9.1	More Details
CVE-2024-11006	Command injection in Ivanti Connect Secure before version 22.7R2.1 (Not Applicable to 9.1Rx) and Ivanti Policy Secure before version 22.7R1.1 (Not Applicable to 9.1Rx) allows a remote authenticated attacker with admin privileges to achieve remote code execution.	9.1	More Details
CVE-2024-11005	Command injection in Ivanti Connect Secure before version 22.7R2.1 (Not Applicable to 9.1Rx) and Ivanti Policy Secure before version 22.7R1.1 (Not Applicable to 9.1Rx) allows a remote authenticated attacker with admin privileges to achieve remote code execution.	9.1	More Details
CVE-2024-10943	An authentication bypass vulnerability exists in the affected product. The vulnerability exists due to shared secrets across accounts and could allow a threat actor to impersonate a user if the threat actor is able to enumerate additional information required during authentication.	9.1	More Details
CVE-2021-35473	An issue was discovered in LemonLDAP::NG before 2.0.12. There is a missing expiration check in the OAuth2.0 handler, i.e., it does not verify access token validity. An attacker can use a expired access token from an OIDC client to access the OAuth2 handler The earliest affected version is 2.0.4.	9.1	More Details
CVE-2024-11007	Command injection in Ivanti Connect Secure before version 22.7R2.1 (Not Applicable to 9.1Rx) and Ivanti Policy Secure before version 22.7R1.1 (Not Applicable to 9.1Rx) allows a remote authenticated attacker with admin privileges to achieve remote code execution.	9.1	More Details
CVE-2024-46890	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 3). The affected application does not properly validate input sent to specific endpoints of its web API. This could allow an authenticated remote attacker with high privileges on the application to execute arbitrary code on the underlying OS.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20457	An issue was discovered on Brother MFC-J491DW C1806180757 devices. The printer's web-interface password hash can be retrieved without authentication, because the response header of any failed login attempt returns an incomplete authorization cookie. The value of the authorization cookie is the MD5 hash of the password in hexadecimal. An attacker can easily derive the true MD5 hash from this, and use offline cracking attacks to obtain administrative access to the device.	9.1	More Details
CVE-2024-51747	Kanboard is project management software that focuses on the Kanban methodology. An authenticated Kanboard admin can read and delete arbitrary files from the server. File attachments, that are viewable or downloadable in Kanboard are resolved through its `path` entry in the `project_has_files` SQLite db. Thus, an attacker who can upload a modified sqlite.db through the dedicated feature, can set arbitrary file links, by abusing path traversals. Once the modified db is uploaded and the project page is accessed, a file download can be triggered and all files, readable in the context of the Kanboard application permissions, can be downloaded. This issue has been addressed in version 1.2.42 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	9.1	More Details
CVE-2024-45765	Dell Enterprise SONiC OS, version(s) 4.1.x, 4.2.x, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution. This is a critical severity vulnerability as it allows high privilege OS commands to be executed with a less privileged role; so Dell recommends customers to upgrade at the earliest opportunity.	9.1	More Details
CVE-2024-43415	An improper neutralization of special elements used in an SQL command in the papertrail/version-model of the decidim_awesome-module <= v0.11.1 (> 0.9.0) allows an authenticated admin user to manipulate sql queries to disclose information, read and write files or execute commands.	9.0	More Details
CVE-2024-45764	Dell Enterprise SONiC OS, version(s) 4.1.x, 4.2.x, contain(s) a Missing Critical Step in Authentication vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Protection mechanism bypass. This is a critical severity vulnerability so Dell recommends customers to upgrade at the earliest opportunity.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-49012	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-48999	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-49004	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-49003	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-11056	A vulnerability, which was classified as critical, was found in Tenda AC10 16.03.10.13. Affected is the function FUN_0046AC38 of the file /goform/WifiExtraSet. The manipulation of the argument wpapsk_crypto leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-49002	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2208	Potential vulnerabilities have been identified in the audio package for certain HP PC products using the Sound Research SECOMN64 driver, which might allow escalation of privilege. Sound Research has released driver updates to mitigate the potential vulnerabilities.	8.8	More Details
CVE-2024-49001	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-49000	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-48998	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-48994	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2019-20458	An issue was discovered on Epson Expression Home XP255 20.08.FM10I8 devices. By default, the device comes (and functions) without a password. The user is at no point prompted to set up a password on the device (leaving a number of devices without a password). In this case, anyone connecting to the web admin panel is capable of becoming admin without using any credentials.	8.8	More Details
CVE-2024-48997	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-48996	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-10827	Use after free in Serial in Google Chrome prior to 130.0.6723.116 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-10826	Use after free in Family Experiences in Google Chrome on Android prior to 130.0.6723.116 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2020-11921	An issue was discovered in Lush 2 through 2020-02-25. Due to the lack of Bluetooth traffic encryption, it is possible to hijack an ongoing Bluetooth connection between the Lush 2 and a mobile phone. This allows an attacker to gain full control over the device.	8.8	More Details
CVE-2024-8069	Limited remote code execution with privilege of a NetworkService Account access in Citrix Session Recording if the attacker is an authenticated user on the same intranet as the session recording server	8.8	More Details
CVE-2024-11048	A vulnerability was found in D-Link DI-8003 16.07.16A1. It has been rated as critical. Affected by this issue is the function dbsrv_asp of the file /dbsrv.asp. The manipulation of the argument str leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-49005	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20536	A vulnerability in a REST API endpoint and web-based management interface of Cisco Nexus Dashboard Fabric Controller (NDFC) could allow an authenticated, remote attacker with read-only privileges to execute arbitrary SQL commands on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a specific REST API endpoint or web-based management interface. A successful exploit could allow the attacker to read, modify, or delete arbitrary data on an internal database, which could affect the availability of the device.	8.8	More Details
CVE-2024-11047	A vulnerability was found in D-Link DI-8003 16.07.16A1. It has been declared as critical. Affected by this vulnerability is the function upgrade_filter_asp of the file /upgrade_filter.asp. The manipulation of the argument path leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-49050	Visual Studio Code Python Extension Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-49039	Windows Task Scheduler Elevation of Privilege Vulnerability	8.8	More Details
CVE-2024-49018	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-49017	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-49016	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-49015	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-49014	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-49013	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-24409	Zohocorp ManageEngine ADManager Plus versions 7203 and prior are vulnerable to Privilege Escalation in the Modify Computers option.	8.8	More Details
CVE-2024-49011	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-49010	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-49009	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49008	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-49007	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-49006	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-48995	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-47590	An unauthenticated attacker can create a malicious link which they can make publicly available. When an authenticated victim clicks on this malicious link, input data will be used by the web site page generation to create content which when executed in the victim's browser (XXS) or transmitted to another server (SSRF) gives the attacker the ability to execute arbitrary code on the server fully compromising confidentiality, integrity and availability.	8.8	More Details
CVE-2024-41992	Wi-Fi Alliance wfa_dut (in Wi-Fi Test Suite) through 9.0.0 allows OS command injection via 802.11x frames because the system() library function is used. For example, on Arcadyan FMIMG51AX000J devices, this leads to wfaTGSendPing remote code execution as root via traffic to TCP port 8000 or 8080 on a LAN interface. On other devices, this may be exploitable over a WAN interface.	8.8	More Details
CVE-2024-43621	Windows Telephony Service Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-11112	Use after free in Media in Google Chrome on Windows prior to 131.0.6778.69 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2024-43628	Windows Telephony Service Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-50809	The theme.php file in SDCMS 2.8 has a command execution vulnerability that allows for the execution of system commands	8.8	More Details
CVE-2024-50329	Path traversal in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote unauthenticated attacker to achieve remote code execution. User interaction is required.	8.8	More Details
CVE-2024-43624	Windows Hyper-V Shared Virtual Disk Elevation of Privilege Vulnerability	8.8	More Details
CVE-2024-43635	Windows Telephony Service Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-11115	Insufficient policy enforcement in Navigation in Google Chrome on iOS prior to 131.0.6778.69 allowed a remote attacker to perform privilege escalation via a series of UI gestures. (Chromium security severity: Medium)	8.8	More Details
CVE-2024-43622	Windows Telephony Service Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46960	The ASD com.rocks.video.downloader (aka HD Video Downloader All Format) application through 7.0.129 for Android allows an attacker to execute arbitrary JavaScript code via the com.rocks.video.downloader.MainBrowserActivity component.	8.8	More Details
CVE-2024-10626	The WooCommerce Support Ticket System plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the delete_uploaded_file() function in all versions up to, and including, 17.7. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	8.8	More Details
CVE-2024-10673	The Top Store theme for WordPress is vulnerable to unauthorized arbitrary plugin installation due to a missing capability check on the top_store_install_and_activate_callback() function in all versions up to, and including, 1.5.4. This makes it possible for authenticated attackers, with subscriber-level access and above, to install arbitrary plugins which can contain other exploitable vulnerabilities to elevate privileges and gain remote code execution.	8.8	More Details
CVE-2024-11061	A vulnerability classified as critical was found in Tenda AC10 16.03.10.13. Affected by this vulnerability is the function FUN_0044db3c of the file /goform/fast_setting_wifi_set. The manipulation of the argument timeZone leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-43620	Windows Telephony Service Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-11113	Use after free in Accessibility in Google Chrome prior to 131.0.6778.69 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2024-43462	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-10674	The Th Shop Mania theme for WordPress is vulnerable to unauthorized arbitrary plugin installation due to a missing capability check on the th_shop_mania_install_and_activate_callback() function in all versions up to, and including, 1.4.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install arbitrary plugins which can be leveraged to exploit other vulnerabilities and achieve remote code execution and privilege escalation.	8.8	More Details
CVE-2024-43459	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2019-20460	An issue was discovered on Epson Expression Home XP255 20.08.FM10I8 devices. POST requests don't require (anti-)CSRF tokens or other mechanisms for validating that the request is from a legitimate source. In addition, CSRF attacks can be used to send text directly to the RAW printer interface. For example, an attack could deliver a worrisome printout to an end user.	8.8	More Details
CVE-2024-50634	A vulnerability in a weak JWT token in Watcharr v1.43.0 and below allows attackers to perform privilege escalation using a crafted JWT token. This vulnerability is not limited to privilege escalation but also affects all functions that require authentication.	8.8	More Details
CVE-2024-38255	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-11017	Webopac from Grand Vice info does not properly validate uploaded file types, allowing remote attackers with regular privileges to upload and execute webshells, which could lead to arbitrary code execution on the server.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21976	Improper input validation in the NPU driver could allow an attacker to supply a specially crafted pointer potentially leading to arbitrary code execution.	8.8	More Details
CVE-2024-21975	Improper input validation in the NPU driver could allow an attacker to supply a specially crafted pointer potentially leading to arbitrary code execution.	8.8	More Details
CVE-2024-48993	SQL Server Native Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-21974	Improper input validation in the NPU driver could allow an attacker to supply a specially crafted pointer potentially leading to arbitrary code execution.	8.8	More Details
CVE-2024-43627	Windows Telephony Service Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-51093	Stored Cross-Site Scripting (XSS) vulnerability in Snipe-IT - v7.0.13 allows an attacker to upload a malicious XML file containing JavaScript code. This can lead to privilege escalation when the payload is executed, granting the attacker super admin permissions within the Snipe-IT system.	8.7	More Details
CVE-2024-10082	CodeChecker is an analyzer tooling, defect database and viewer extension for the Clang Static Analyzer and Clang Tidy. Authentication method confusion allows logging in as the built-in root user from an external service. The built-in root user up until 6.24.1 is generated in a weak manner, cannot be disabled, and has universal access.This vulnerability allows an attacker who can create an account on an enabled external authentication service, to log in as the root user, and access and control everything that can be controlled via the web interface. The attacker needs to acquire the username of the root user to be successful. This issue affects CodeChecker: through 6.24.1.	8.7	More Details
CVE-2024-52007	HAPI FHIR is a complete implementation of the HL7 FHIR standard for healthcare interoperability in Java. XSLT parsing performed by various components are vulnerable to XML external entity injections. A processed XML file with a malicious DTD tag (<!DOCTYPE foo [<!ENTITY example SYSTEM "/etc/passwd">]> could produce XML containing data from the host system. This impacts use cases where org.hl7.fhir.core is being used to within a host where external clients can submit XML. This is related to GHSA-6cr6-ph3p-f5rf, in which its fix (#1571 & #1717) was incomplete. This issue has been addressed in release version 6.4.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	8.6	More Details
CVE-2024-51998	changedetection.io is a free open source web page change detection tool. The validation for the file URI scheme falls short, and results in an attacker being able to read any file on the system. This issue only affects instances with a webdriver enabled, and `ALLOW_FILE_URI` false or not defined. The check used for URL protocol, `is_safe_url`, allows `file:` as a URL scheme. It later checks if local files are permitted, but one of the preconditions for the check is that the URL starts with `file://`. The issue comes with the fact that the file URI scheme is not required to have double slashes. This issue has been addressed in version 0.47.06 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	8.6	More Details
CVE-2024-38286	Allocation of Resources Without Limits or Throttling vulnerability in Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M20, from 10.1.0-M1 through 10.1.24, from 9.0.13 through 9.0.89. Older, unsupported versions may also be affected. Users are recommended to upgrade to version 11.0.0-M21, 10.1.25, or 9.0.90, which fixes the issue. Apache Tomcat, under certain configurations on any platform, allows an attacker to cause an OutOfMemoryError by abusing the TLS handshake process.	8.6	More Details
CVE-2024-51602	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Oleksandr Ustymenko Simple Job Manager allows SQL Injection.This issue affects Simple Job Manager: from n/a through 1.1.	8.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50544	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Micah Blu RSVP ME allows SQL Injection.This issue affects RSVP ME: from n/a through 1.9.9.	8.5	More Details
CVE-2024-50539	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Lodgix Lodgix.Com Vacation Rental Website Builder allows SQL Injection.This issue affects Lodgix.Com Vacation Rental Website Builder: from n/a through 3.9.73.	8.5	More Details
CVE-2024-50524	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in quyle91 Administrator Z allows Blind SQL Injection.This issue affects Administrator Z: from n/a through 2024.11.04.	8.5	More Details
CVE-2024-51625	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in EDC Team (E-Da`wah Committee) Quran Shortcode allows Blind SQL Injection.This issue affects Quran Shortcode: from n/a through 1.5.	8.5	More Details
CVE-2024-51621	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Reza Sh Download-Mirror-Counter allows SQL Injection.This issue affects Download-Mirror-Counter: from n/a through 1.1.	8.5	More Details
CVE-2024-50386	Account users in Apache CloudStack by default are allowed to register templates to be downloaded directly to the primary storage for deploying instances. Due to missing validation checks for KVM-compatible templates in CloudStack 4.0.0 through 4.18.2.4 and 4.19.0.0 through 4.19.1.2, an attacker that can register templates, can use them to deploy malicious instances on KVM-based environments and exploit this to gain access to the host filesystems that could result in the compromise of resource integrity and confidentiality, data loss, denial of service, and availability of KVM-based infrastructure managed by CloudStack. Users are recommended to upgrade to Apache CloudStack 4.18.2.5 or 4.19.1.3, or later, which addresses this issue. Additionally, all user-registered KVM-compatible templates can be scanned and checked that they are flat files that should not be using any additional or unnecessary features. For example, operators can run the following command on their file-based primary storage(s) and inspect the output. An empty output for the disk being validated means it has no references to the host filesystems; on the other hand, if the output for the disk being validated is not empty, it might indicate a compromised disk. However, bear in mind that (i) volumes created from templates will have references for the templates at first and (ii) volumes can be consolidated while migrating, losing their references to the templates. Therefore, the command execution for the primary storages can show both false positives and false negatives. for file in $(find /path/to/storage/ -type f -regex [a-f0-9\-]*.*); do echo "Retrieving file [$file] info. If the output is not empty, that might indicate a compromised disk; check it carefully."; qemu-img info -U $file l grep file: ; printf "\n\n"; done For checking the whole template/volume features of each disk, operators can run the following command: for file in $(find /path/to/storage/ -type f -regex [a-f0-9\-]*.*); do echo "Retrieving file [$file] info."; qemu-img info -U $file; printf "\n\n"; done	8.5	More Details
CVE-2024-51570	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Odihost Easy Gallery allows SQL Injection.This issue affects Easy Gallery: from n/a through 1.4.	8.5	More Details
CVE-2024-51579	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Saleswonder.Biz 5 Stars Rating Funnel allows SQL Injection.This issue affects 5 Stars Rating Funnel: from n/a through 1.4.01.	8.5	More Details
CVE-2024-51601	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Maksym Marko Website price calculator allows SQL Injection.This issue affects Website price calculator: from n/a through 4.1.	8.5	More Details
CVE-2024-51620	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Porsline allows Blind SQL Injection.This issue affects Porsline: from n/a through 1.0.2.	8.5	More Details
CVE-2024-51607	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Buddy Lindsey Golf Tracker allows SQL Injection.This issue affects Golf Tracker: from n/a through 0.7.	8.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51619	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Market360.Co Market 360 Viewer allows Blind SQL Injection.This issue affects Market 360 Viewer: from n/a through 1.01.	8.5	More Details
CVE-2024-10839	Zohocorp ManageEngine SharePoint Manager Plus versions 4503 and prior are vulnerable to authenticated XML External Entity (XXE) in the Management option.	8.5	More Details
CVE-2024-51837	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in SONS Creative Development WP Contest allows SQL Injection.This issue affects WP Contest: from n/a through 1.0.0.	8.5	More Details
CVE-2024-51845	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Richteam Share Buttons – Social Media allows Blind SQL Injection.This issue affects Share Buttons – Social Media: from n/a through 1.0.2.	8.5	More Details
CVE-2024-51606	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Blrt Blrt WP Embed allows SQL Injection.This issue affects Blrt WP Embed: from n/a through 1.6.9.	8.5	More Details
CVE-2024-51843	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Olland.Biz Horsemanager allows Blind SQL Injection.This issue affects Horsemanager: from n/a through 1.3.	8.5	More Details
CVE-2024-51820	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in L Squared Support L Squared Hub WP allows SQL Injection.This issue affects L Squared Hub WP: from n/a through 1.0.	8.5	More Details
CVE-2024-51608	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Pluginhandy AmaDiscount allows SQL Injection.This issue affects AmaDiscount: from n/a through 1.0.	8.5	More Details
CVE-2024-51882	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ehues Gboy Custom Google Map allows Blind SQL Injection.This issue affects Gboy Custom Google Map: from n/a through 1.2.	8.5	More Details
CVE-2024-51623	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mehrdad Farahani WP EIS allows SQL Injection.This issue affects WP EIS: from n/a through 1.3.3.	8.5	More Details
CVE-2024-47808	A vulnerability has been identified in SINEC NMS (All versions < V3.0 SP1). The affected application contains a database function, that does not properly restrict the permissions of users to write to the filesystem of the host system. This could allow an authenticated medium-privileged attacker to write arbitrary content to any location in the filesystem of the host system.	8.4	More Details
CVE-2024-52531	GNOME libsoup before 3.6.1 allows a buffer overflow in applications that perform conversion to UTF-8 in soup_header_parse_param_list_strict. Input received over the network cannot trigger this.	8.4	More Details
CVE-2024-10944	A Remote Code Execution vulnerability exists in the affected product. The vulnerability requires a high level of permissions and exists due to improper input validation resulting in the possibility of a malicious Updated Agent being deployed.	8.4	More Details
CVE-2024-27529	wasm3 139076a contains memory leaks in Read_utf8.	8.4	More Details
CVE-2024-27528	wasm3 139076a suffers from Invalid Memory Read, leading to DoS and potential Code Execution.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20459	An issue was discovered on Epson Expression Home XP255 20.08.FM10I8 devices. With the SNMPv1 public community, all values can be read, and with the epson community, all the changeable values can be written/updated, as demonstrated by permanently disabling the network card or changing the DNS servers.	8.4	More Details
CVE-2024-45794	devtron is an open source tool integration platform for Kubernetes. In affected versions an authenticated user (with minimum permission) could utilize and exploit SQL Injection to allow the execution of malicious SQL queries via CreateUser API (/orchestrator/user). This issue has been addressed in version 0.7.2 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	8.3	More Details
CVE-2024-11114	Inappropriate implementation in Views in Google Chrome on Windows prior to 131.0.6778.69 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	8.3	More Details
CVE-2024-36513	A privilege context switching error vulnerability [CWE-270] in FortiClient Windows version 7.2.4 and below, version 7.0.12 and below, 6.4 all versions may allow an authenticated user to escalate their privileges via lua auto patch scripts.	8.2	More Details
CVE-2024-51487	Ampache is a web based audio/video streaming application and file manager. The current implementation of token parsing fails to properly validate CSRF tokens when activating or deactivating catalog. This vulnerability allows an attacker to exploit CSRF attacks, potentially enabling them to change website features that should only be managed by administrators through malicious requests. This issue has been addressed in version 7.0.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	8.1	More Details
CVE-2024-46966	The Ikhgur mn.ikhgur.khotoch (aka Video Downloader Pro & Browser) application through 1.0.42 for Android allows an attacker to execute arbitrary JavaScript code via the mn.ikhgur.khotoch.MainActivity component.	8.1	More Details
CVE-2024-46961	The Inshot com.downloader.privatebrowser (aka Video Downloader - XDownloader) application through 1.3.5 for Android allows an attacker to execute arbitrary JavaScript code via the com.downloader.privatebrowser.activity.PrivateMainActivity component.	8.1	More Details
CVE-2024-46963	The com.superfast.video.downloader (aka Super Unlimited Video Downloader - All in One) application through 5.1.9 for Android allows an attacker to execute arbitrary JavaScript code via the com.bluesky.browser.ui.BrowserMainActivity component.	8.1	More Details
CVE-2024-10020	The Heateor Social Login WordPress plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 1.1.35. This is due to insufficient verification on the user being returned by the social login token. This makes it possible for unauthenticated attackers to log in as any existing user on the site, if they have access to the email and the user does not have an already-existing account for the service returning the token. An attacker cannot authenticate as an administrator by default, but these accounts are also at risk if authentication for administrators has explicitly been allowed via the social login.	8.1	More Details
CVE-2024-43425	A flaw was found in Moodle. Additional restrictions are required to avoid a remote code execution risk in calculated question types. Note: This requires the capability to add/update questions.	8.1	More Details
CVE-2024-43625	Microsoft Windows VMSwitch Elevation of Privilege Vulnerability	8.1	More Details
CVE-2024-46964	The com.video.downloader.all (aka All Video Downloader) application through 11.28 for Android allows an attacker to execute arbitrary JavaScript code via the com.video.downloader.all.StartActivity component.	8.1	More Details
CVE-2024-43434	The bulk message sending feature in Moodle's Feedback module's non-respondents report had an incorrect CSRF token check, leading to a CSRF vulnerability.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51484	Ampache is a web based audio/video streaming application and file manager. The current implementation of token parsing fails to properly validate CSRF tokens when activating or deactivating controllers. This vulnerability allows an attacker to exploit CSRF attacks, potentially enabling them to change website features that should only be managed by administrators through malicious requests. This issue has been addressed in version 7.0.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	8.1	More Details
CVE-2024-48325	Portabilis i-Educar 2.8.0 is vulnerable to SQL Injection in the "getDocuments" function of the "InstituicaoDocumentacaoController" class. The "instituicao_id" parameter in "/module/Api/InstituicaoDocumentacao?oper=get&resource=getDocuments&instituicao_id" is not properly sanitized, allowing an unauthenticated remote attacker to inject malicious SQL commands.	8.1	More Details
CVE-2024-9946	The Social Share, Social Login and Social Comments Plugin – Super Socializer plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 7.13.68. This is due to insufficient verification on the user being returned by the social login token. This makes it possible for unauthenticated attackers to log in as any existing user on the site, if they have access to the email and the user does not have an already-existing account for the service returning the token. An attacker cannot authenticate as an administrator by default, but these accounts are also at risk if authentication for administrators has explicitly been allowed via the social login. The vulnerability was partially patched in version 7.13.68.	8.1	More Details
CVE-2024-43598	LightGBM Remote Code Execution Vulnerability	8.1	More Details
CVE-2024-10914	A vulnerability was found in D-Link DNS-320, DNS-320LW, DNS-325 and DNS-340L up to 20241028. It has been declared as critical. Affected by this vulnerability is the function cgi_user_add of the file /cgi-bin/account_mgr.cgi?cmd=cgi_user_add. The manipulation of the argument name leads to os command injection. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used.	8.1	More Details
CVE-2024-10915	A vulnerability was found in D-Link DNS-320, DNS-320LW, DNS-325 and DNS-340L up to 20241028. It has been rated as critical. Affected by this issue is the function cgi_user_add of the file /cgi-bin/account_mgr.cgi?cmd=cgi_user_add. The manipulation of the argument group leads to os command injection. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used.	8.1	More Details
CVE-2024-51485	Ampache is a web based audio/video streaming application and file manager. The current implementation of token parsing fails to properly validate CSRF tokens when activating or deactivating plugins. This vulnerability allows an attacker to exploit CSRF attacks, potentially enabling them to change website features that should only be managed by administrators through malicious requests. This issue has been addressed in version 7.0.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	8.1	More Details
CVE-2024-51997	Trustee is a set of tools and components for attesting confidential guests and providing secrets to them. The ART (**Attestation Results Token**) token, generated by AS, could be manipulated by MITM attacker, but the verifier (CoCo Verification Demander like KBS) could still verify it successfully. In the payload of ART token, the ‘jwk’ could be replaced by attacker with his own pub key. Then attacker can use his own corresponding private key to sign the crafted ART token. Based on current code implementation (v0.8.0), such replacement and modification can not be detected. This issue has been addressed in version 0.8.2 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	8.1	More Details
CVE-2024-43447	Windows SMBv3 Server Remote Code Execution Vulnerability	8.1	More Details
CVE-2024-49048	TorchGeo Remote Code Execution Vulnerability	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48322	UsersController.php in Run.codes 1.5.2 and older has a reset password race condition vulnerability.	8.1	More Details
CVE-2024-51094	An issue in Snipe-IT v.7.0.13 build 15514 allows a low-privileged attacker to modify their profile name and inject a malicious payload into the "Name" field. When an administrator later accesses the People Management page, exports the data as a CSV file, and opens it, the injected payload will be executed, allowing the attacker to exfiltrate internal system data from the CSV file to a remote server.	8.0	More Details
CVE-2024-45827	Improper neutralization of special elements used in an OS command ('OS Command Injection') issue exists in Mesh Wi-Fi router RP562B firmware version v1.0.2 and earlier. If this vulnerability is exploited, a network-adjacent authenticated attacker may execute an arbitrary OS command.	8.0	More Details
CVE-2024-28726	An issue in DLink DWR 2000M 5G CPE With Wifi 6 Ax1800 and Dlink DWR 5G CPE DWR-2000M_1.34ME allows a local attacker to execute arbitrary code via a crafted payload to the Diagnostics function.	8.0	More Details
CVE-2024-51186	D-Link DIR-820L 1.05b03 was discovered to contain a remote code execution (RCE) vulnerability via the ping_addr parameter in the ping_v4 and ping_v6 functions.	8.0	More Details
CVE-2024-24914	Authenticated Gaia users can inject code or commands by global variables through special HTTP requests. A Security fix that mitigates this vulnerability is available.	8.0	More Details
CVE-2020-11919	An issue was discovered in Siime Eye 14.1.00000001.3.330.0.0.3.14. There is no CSRF protection.	8.0	More Details
CVE-2024-8424	Improper Privilege Management vulnerability in WatchGuard EPDR, Panda AD360 and Panda Dome on Windows (PSANHost.exe module) allows arbitrary file delete with SYSTEM permissions. This issue affects EPDR: before 8.00.23.0000; Panda AD360: before 8.00.23.0000; Panda Dome: before 22.03.00.	7.8	More Details
CVE-2024-49517	Substance3D - Painter versions 10.1.0 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-49516	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-47906	Excessive binary privileges in Ivanti Connect Secure before version 22.7R2.3 (Not Applicable to 9.1Rx) and Ivanti Policy Secure before version 22.7R1.2 (Not Applicable to 9.1Rx) allows a local authenticated attacker to escalate privileges.	7.8	More Details
CVE-2024-43636	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-49520	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-43641	Windows Registry Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-50322	Path traversal in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a local unauthenticated attacker to achieve code execution. User interaction is required.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43644	Windows Client-Side Caching Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-43640	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-49518	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-49525	Substance3D - Painter versions 10.1.0 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-49519	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-43629	Windows DWM Core Library Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-50323	SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a local unauthenticated attacker to achieve code execution. User interaction is required.	7.8	More Details
CVE-2024-35423	vmir e8117 was discovered to contain a heap buffer overflow via the wasm_parse_section_functions function at /src/vmir_wasm_parser.c.	7.8	More Details
CVE-2024-50209	In the Linux kernel, the following vulnerability has been resolved: RDMA/bnxt_re: Add a check for memory allocation __alloc_pbl() can return error when memory allocation fails. Driver is not checking the status on one of the instances.	7.8	More Details
CVE-2024-50590	Attackers with local access to the medical office computer can escalate their Windows user privileges to "NT AUTHORITY\SYSTEM" by overwriting one of two Elefant service binaries with weak permissions. The default installation directory of Elefant is "C:\Elefant1" which is writable for all users. In addition, the Elefant installer registers two Firebird database services which are running as “NT AUTHORITY\SYSTEM”. Path: C:\Elefant1\Firebird_2\bin\fbserver.exe Path: C:\Elefant1\Firebird_2\bin\fbguard.exe Both service binaries are user writable. This means that a local attacker can rename one of the service binaries, replace the service executable with a new executable, and then restart the system. Once the system has rebooted, the new service binary is executed as "NT AUTHORITY\SYSTEM".	7.8	More Details
CVE-2024-50591	An attacker with local access the to medical office computer can escalate his Windows user privileges to "NT AUTHORITY\SYSTEM" by exploiting a command injection vulnerability in the Elefant Update Service. The command injection can be exploited by communicating with the Elefant Update Service which is running as "SYSTEM" via Windows Named Pipes.The Elefant Software Updater (ESU) consists of two components. An ESU service which runs as "NT AUTHORITY\SYSTEM" and an ESU tray client which communicates with the service to update or repair the installation and is running with user permissions. The communication is implemented using named pipes. A crafted message of type "MessageType.SupportServiceInfos" can be sent to the local ESU service to inject commands, which are then executed as "NT AUTHORITY\SYSTEM".	7.8	More Details
CVE-2024-47131	If an attacker tricks a valid user into running Delta Electronics DIAScreen with a file containing malicious code, a stack-based buffer overflow in BACnetObjectInfo can be exploited, allowing the attacker to remotely execute arbitrary code.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50203	In the Linux kernel, the following vulnerability has been resolved: bpf, arm64: Fix address emission with tag-based KASAN enabled When BPF_TRAMP_F_CALL_ORIG is enabled, the address of a bpf_tramp_image struct on the stack is passed during the size calculation pass and an address on the heap is passed during code generation. This may cause a heap buffer overflow if the heap address is tagged because emit_a64_mov_i64() will emit longer code than it did during the size calculation pass. The same problem could occur without tag-based KASAN if one of the 16-bit words of the stack address happened to be all-ones during the size calculation pass. Fix the problem by assuming the worst case (4 instructions) when calculating the size of the bpf_tramp_image address emission.	7.8	More Details
CVE-2024-50593	An attacker with local access to the medical office computer can access restricted functions of the Elefant Service tool by using a hard-coded "Hotline" password in the Elefant service binary, which is shipped with the software.	7.8	More Details
CVE-2024-25431	An issue in bytecodealliance wasm-micro-runtime before v.b3f728c and fixed in commit 06df58f allows a remote attacker to escalate privileges via a crafted file to the check_was_abi_compatibility function.	7.8	More Details
CVE-2024-7571	Incorrect permissions in Ivanti Secure Access Client before 22.7R4 allows a local authenticated attacker to escalate their privileges.	7.8	More Details
CVE-2024-49528	Animate versions 23.0.7, 24.0.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-39354	If an attacker tricks a valid user into running Delta Electronics DIAScreen with a file containing malicious code, a stack-based buffer overflow in CEtherIPTagItem can be exploited, allowing the attacker to remotely execute arbitrary code.	7.8	More Details
CVE-2024-49526	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-43530	Windows Update Stack Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-49509	InDesign Desktop versions ID18.5.3, ID19.5 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-49508	InDesign Desktop versions ID18.5.2, ID19.5 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-50186	In the Linux kernel, the following vulnerability has been resolved: net: explicitly clear the sk pointer, when pf->create fails We have recently noticed the exact same KASAN splat as in commit 6cd4a78d962b ("net: do not leave a dangling sk pointer, when socket creation fails"). The problem is that commit did not fully address the problem, as some pf->create implementations do not use sk_common_release in their error paths. For example, we can use the same reproducer as in the above commit, but changing ping to arping. arping uses AF_PACKET socket and if packet_create fails, it will just sk_free the allocated sk object. While we could chase all the pf->create implementations and make sure they NULL the freed sk object on error from the socket, we can't guarantee future protocols will not make the same mistake. So it is easier to just explicitly NULL the sk pointer upon return from pf->create in __sock_create. We do know that pf->create always releases the allocated sk object on error, so if the pointer is not NULL, it is definitely dangling.	7.8	More Details
CVE-2024-49507	InDesign Desktop versions ID18.5.2, ID19.5 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43623	Windows NT OS Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-43626	Windows Telephony Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-50180	In the Linux kernel, the following vulnerability has been resolved: fbdev: sisfb: Fix strbuf array overflow The values of the variables xres and yres are placed in strbuf. These variables are obtained from strbuf1. The strbuf1 array contains digit characters and a space if the array contains non-digit characters. Then, when executing sprintf(strbuf, "%ux%ux8", xres, yres); more than 16 bytes will be written to strbuf. It is suggested to increase the size of the strbuf array to 24. Found by Linux Verification Center (linuxtesting.org) with SVACE.	7.8	More Details
CVE-2024-43630	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-49514	Photoshop Desktop versions 24.7.3, 25.11 and earlier are affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-48837	Dell SmartFabric OS10 Software, version(s) 10.5.6.x, 10.5.5.x, 10.5.4.x, 10.5.3.x, contain(s) an Execution with Unnecessary Privileges vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Command execution	7.8	More Details
CVE-2024-50257	In the Linux kernel, the following vulnerability has been resolved: netfilter: Fix use-after-free in get_info() ip6table_nat module unload has refcnt warning for UAF. call trace is: WARNING: CPU: 1 PID: 379 at kernel/module/main.c:853 module_put+0x6f/0x80 Modules linked in: ip6table_nat(-) CPU: 1 UID: 0 PID: 379 Comm: ip6tables Not tainted 6.12.0-rc4-00047-gc2ee9f594da8-dirty #205 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.13.0-0-gf21b5a4aeb02-prebuilt.qemu.org 04/01/2014 RIP: 0010:module_put+0x6f/0x80 Call Trace: <TASK> get_info+0x128/0x180 do_ip6t_get_ctl+0x6a/0x430 nf_getsockopt+0x46/0x80 ipv6_getsockopt+0xb9/0x100 rawv6_getsockopt+0x42/0x190 do_sock_getsockopt+0xaa/0x180 __sys_getsockopt+0x70/0xc0 __x64_sys_getsockopt+0x20/0x30 do_syscall_64+0xa2/0x1a0 entry_SYSCALL_64_after_hwframe+0x77/0x7f Concurrent execution of module unload and get_info() trigered the warning. The root cause is as follows: cpu0 cpu1 module_exit //mod->state = MODULE_STATE_GOING ip6table_nat_exit xt_unregister_template kfree(t) //removed from templ_list getinfo() t = xt_find_table_lock list_for_each_entry(tmpl, &xt_templates[af]...) if (strcmp(tmpl->name, name)) continue; //table not found try_module_get list_for_each_entry(t, &xt_net->tables[af]...) return t; //not get refcnt module_put(t->me) //uaf unregister_pernet_subsys //remove table from xt_net list While xt_table module was going away and has been removed from xt_templates list, we couldnt get refcnt of xt_table->me. Check module in xt_net->tables list re-traversal to fix it.	7.8	More Details
CVE-2024-46956	An issue was discovered in psi/zfile.c in Artifex Ghostscript before 10.04.0. Out-of-bounds data access in filenameforall can lead to arbitrary code execution.	7.8	More Details
CVE-2024-49028	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-49026	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-49021	Microsoft SQL Server Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50150	In the Linux kernel, the following vulnerability has been resolved: usb: typec: altmode should keep reference to parent The altmode device release refers to its parent device, but without keeping a reference to it. When registering the altmode, get a reference to the parent and put it in the release function. Before this fix, when using CONFIG_DEBUG_KOBJECT_RELEASE, we see issues like this: [43.572860] kobject: 'port0.0' (ffff8880057ba008): kobject_release, parent 0000000000000000 (delayed 3000) [43.573532] kobject: 'port0.1' (ffff8880057bd008): kobject_release, parent 0000000000000000 (delayed 1000) [43.574407] kobject: 'port0' (ffff8880057b9008): kobject_release, parent 0000000000000000 (delayed 3000) [43.575059] kobject: 'port1.0' (ffff8880057ca008): kobject_release, parent 0000000000000000 (delayed 4000) [43.575908] kobject: 'port1.1' (ffff8880057c9008): kobject_release, parent 0000000000000000 (delayed 4000) [43.576908] kobject: 'typec' (ffff8880062dbc00): kobject_release, parent 0000000000000000 (delayed 4000) [43.577769] kobject: 'port1' (ffff8880057bf008): kobject_release, parent 0000000000000000 (delayed 3000) [46.612867] == [46.613402] BUG: KASAN: slab-use-after-free in typec_altmode_release+0x38/0x129 [46.614003] Read of size 8 at addr ffff8880057b9118 by task kworker/2:1/48 [46.614538] [46.614668] CPU: 2 UID: 0 PID: 48 Comm: kworker/2:1 Not tainted 6.12.0-rc1-00138-gedbae730ad31 #535 [46.615391] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.15.0-1 04/01/2014 [46.616042] Workqueue: events kobject_delayed_cleanup [46.616446] Call Trace: [46.616648] <TASK> [46.616820] dump_stack_lvl+0x5b/0x7c [46.617112] ? typec_altmode_release+0x38/0x129 [46.617470] print_report+0x14c/0x49e [46.617769] ? rcu_read_unlock_sched+0x56/0x69 [46.618117] ? __virt_addr_valid+0x19a/0x1ab [46.618456] ? kmem_cache_debug_flags+0xc/0x1d [46.618807] ? typec_altmode_release+0x38/0x129 [46.619161] kasan_report+0x8d/0xb4 [46.619447] ? typec_altmode_release+0x38/0x129 [46.619809] ? process_scheduled_works+0x3cb/0x85f [46.620185] typec_altmode_release+0x38/0x129 [46.620537] ? process_scheduled_works+0x3cb/0x85f [46.620907] device_release+0xaf/0xf2 [46.621206] kobject_delayed_cleanup+0x13b/0x17a [46.621584] process_scheduled_works+0x4f6/0x85f [46.621955] ? __pfx_process_scheduled_works+0x10/0x10 [46.622353] ? hlock_class+0x31/0x9a [46.622647] ? lock_acquired+0x361/0x3c3 [46.622956] ? move_linked_works+0x46/0x7d [46.623277] worker_thread+0x1ce/0x291 [46.623582] ? __kthread_parkme+0xc8/0xdf [46.623900] ? __pfx_worker_thread+0x10/0x10 [46.624236] kthread+0x17e/0x190 [46.624501] ? kthread+0xfb/0x190 [46.624756] ? __pfx_kthread+0x10/0x10 [46.625015] ret_from_fork+0x20/0x40 [46.625268] ? __pfx_kthread+0x10/0x10 [46.625532] ret_from_fork_asm+0x1a/0x30 [46.625805] </TASK> [46.625953] [46.626056] Allocated by task 678: [46.626287] kasan_save_stack+0x24/0x44 [46.626555] kasan_save_track+0x14/0x2d [46.626811] __kasan_kmalloc+0x3f/0x4d [46.627049] __kmalloc_noprof+0x1bf/0x1f0 [46.627362] typec_register_port+0x23/0x491 [46.627698] cros_typec_probe+0x634/0xbb6 [46.628026] platform_probe+0x47/0x8c [46.628311] really_probe+0x20a/0x47d [46.628605] device_driver_attach+0x39/0x72 [46.628940] bind_store+0x87/0xd7 [46.629213] kernfs_fop_write_iter+0x1aa/0x218 [46.629574] vfs_write+0x1d6/0x29b [46.629856] ksys_write+0xcd/0x13b [46.630128] do_syscall_64+0xd4/0x139 [46.630420] entry_SYSCALL_64_after_hwframe+0x76/0x7e [46.630820] [46.630946] Freed by task 48: [46.631182] kasan_save_stack+0x24/0x44 [46.631493] kasan_save_track+0x14/0x2d [46.631799] kasan_save_free_info+0x3f/0x4d [46.632144] __kasan_slab_free+0x37/0x45 [46.632474] ---truncated---	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50151	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix OOBs when building SMB2_IOCTL request When using encryption, either enforced by the server or when using 'seal' mount option, the client will squash all compound request buffers down for encryption into a single iov in smb2_set_next_command(). SMB2_ioctl_init() allocates a small buffer (448 bytes) to hold the SMB2_IOCTL request in the first iov, and if the user passes an input buffer that is greater than 328 bytes, smb2_set_next_command() will end up writing off the end of @rqst->iov[0].iov_base as shown below: mount.cifs //srv/share /mnt -o ...,seal ln -s $(perl -e "print('a')for 1..1024") /mnt/link BUG: KASAN: slab-out-of-bounds in smb2_set_next_command.cold+0x1d6/0x24c [cifs] Write of size 4116 at addr ffff8881148fcab8 by task ln/859 CPU: 1 UID: 0 PID: 859 Comm: ln Not tainted 6.12.0-rc3 #1 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-2.fc40 04/01/2014 Call Trace: <TASK> dump_stack_lvl+0x5d/0x80 ? smb2_set_next_command.cold+0x1d6/0x24c [cifs] print_report+0x156/0x4d9 ? smb2_set_next_command.cold+0x1d6/0x24c [cifs] ? __virt_addr_valid+0x145/0x310 ? __phys_addr+0x46/0x90 ? smb2_set_next_command.cold+0x1d6/0x24c [cifs] kasan_report+0xda/0x110 ? smb2_set_next_command.cold+0x1d6/0x24c [cifs] kasan_check_range+0x10f/0x1f0 __asan_memcpy+0x3c/0x60 smb2_set_next_command.cold+0x1d6/0x24c [cifs] smb2_compound_op+0x238c/0x3840 [cifs] ? kasan_save_track+0x14/0x30 ? kasan_save_free_info+0x3b/0x70 ? vfs_symlink+0x1a1/0x2c0 ? do_symlinkat+0x108/0x1c0 ? __pfx_smb2_compound_op+0x10/0x10 [cifs] ? kmem_cache_free+0x118/0x3e0 ? cifs_get_writable_path+0xeb/0x1a0 [cifs] smb2_get_reparse_inode+0x423/0x540 [cifs] ? __pfx_smb2_get_reparse_inode+0x10/0x10 [cifs] ? rcu_is_watching+0x20/0x50 ? __kmalloc_noprof+0x37c/0x480 ? smb2_create_reparse_symlink+0x257/0x490 [cifs] ? smb2_create_reparse_symlink+0x38f/0x490 [cifs] smb2_create_reparse_symlink+0x38f/0x490 [cifs] ? __pfx_smb2_create_reparse_symlink+0x10/0x10 [cifs] ? find_held_lock+0x8a/0xa0 ? hlock_class+0x32/0xb0 ? __build_path_from_dentry_optional_prefix+0x19d/0x2e0 [cifs] cifs_symlink+0x24f/0x960 [cifs] ? __pfx_make_vfsuid+0x10/0x10 ? __pfx_cifs_symlink+0x10/0x10 [cifs] ? make_vfsgid+0x6b/0xc0 ? generic_permission+0x96/0x2d0 vfs_symlink+0x1a1/0x2c0 do_symlinkat+0x108/0x1c0 ? __pfx_do_symlinkat+0x10/0x10 ? strncpy_from_user+0xaa/0x160 __x64_sys_symlinkat+0xb9/0xf0 do_syscall_64+0xbb/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f08d75c13bb	7.8	More Details
CVE-2024-49019	Active Directory Certificate Services Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-50230	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix kernel bug due to missing clearing of checked flag Syzbot reported that in directory operations after nilfs2 detects filesystem corruption and degrades to read-only, __block_write_begin_int(), which is called to prepare block writes, may fail the BUG_ON check for accesses exceeding the folio/page size, triggering a kernel bug. This was found to be because the "checked" flag of a page/folio was not cleared when it was discarded by nilfs2's own routine, which causes the sanity check of directory entries to be skipped when the directory page/folio is reloaded. So, fix that. This was necessary when the use of nilfs2's own page discard routine was applied to more than just metadata files.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50155	In the Linux kernel, the following vulnerability has been resolved: netdevsim: use cond_resched() in nsim_dev_trap_report_work() I am still seeing many syzbot reports hinting that syzbot might fool nsim_dev_trap_report_work() with hundreds of ports [1] Lets use cond_resched(), and system_unbound_wq instead of implicit system_wq. [1] INFO: task syz-executor:20633 blocked for more than 143 seconds. Not tainted 6.12.0-rc2-syzkaller-00205-g1d227fcc7222 #0 "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message. task:syz-executor state:D stack:25856 pid:20633 tgid:20633 ppid:1 flags:0x00004006 ... NMI backtrace for cpu 1 CPU: 1 UID: 0 PID: 16760 Comm: kworker/1:0 Not tainted 6.12.0-rc2-syzkaller-00205-g1d227fcc7222 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 09/13/2024 Workqueue: events nsim_dev_trap_report_work RIP: 0010:__sanitizer_cov_trace_pc+0x0/0x70 kernel/kcov.c:210 Code: 89 fb e8 23 00 00 00 48 8b 3d 04 fb 9c 0c 48 89 de 5b e9 c3 c7 5d 00 0f 1f 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 <f3> 0f 1e fa 48 8b 04 24 65 48 8b 0c 25 c0 d7 03 00 65 8b 15 60 f0 RSP: 0018:ffffc90000a187e8 EFLAGS: 00000246 RAX: 0000000000000100 RBX: ffffc90000a188e0 RCX: ffff888027d3bc00 RDX: ffff888027d3bc00 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffff88804a2e6000 R08: ffffffff8a4bc495 R09: ffffffff89da3577 R10: 0000000000000004 R11: ffffffff8a4bc2b0 R12: dfffffc0000000000 R13: ffff88806573b503 R14: dfffffc0000000000 R15: ffff8880663cca00 FS: 0000000000000000(0000) GS:ffff8880b8700000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fc90a747f98 CR3: 000000000e734000 CR4: 00000000003526f0 DR0: 0000000000000000 DR1: 0000000000000002b DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000ffff0ff0 DR7: 0000000000000400 Call Trace: <NMI> </NMI> <TASK> __local_bh_enable_ip+0x1bb/0x200 kernel/softirq.c:382 spin_unlock_bh include/linux/spinlock.h:396 [inline] nsim_dev_trap_report drivers/net/netdevsim/dev.c:820 [inline] nsim_dev_trap_report_work+0x75d/0xaa0 drivers/net/netdevsim/dev.c:850 process_one_work kernel/workqueue.c:3229 [inline] process_scheduled_works+0xa63/0x1850 kernel/workqueue.c:3310 worker_thread+0x870/0xd30 kernel/workqueue.c:3391 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 </TASK>	7.8	More Details
CVE-2024-50158	In the Linux kernel, the following vulnerability has been resolved: RDMA/bnxt_re: Fix out of bound check Driver exports pacing stats only on GenP5 and P7 adapters. But while parsing the pacing stats, driver has a check for "rdev->dbr_pacing". This caused a trace when KASAN is enabled. BUG: KASAN: slab-out-of-bounds in bnxt_re_get_hw_stats+0x2b6a/0x2e00 [bnxt_re] Write of size 8 at addr ffff8885942a6340 by task modprobe/4809	7.8	More Details
CVE-2024-50159	In the Linux kernel, the following vulnerability has been resolved: firmware: arm_scmi: Fix the double free in scmi_debugfs_common_setup() Clang static checker(scan-build) throws below warning： l drivers/firmware/arm_scmi/driver.c:line 2915, column 2 l Attempt to free released memory. When devm_add_action_or_reset() fails, scmi_debugfs_common_cleanup() will run twice which causes double free of 'dbg->name'. Remove the redundant scmi_debugfs_common_cleanup() to fix this problem.	7.8	More Details
CVE-2024-45114	Illustrator versions 28.7.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-47441	After Effects versions 23.6.9, 24.6.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50226	In the Linux kernel, the following vulnerability has been resolved: cxl/port: Fix use-after-free, permit out-of-order decoder shutdown In support of investigating an initialization failure report [1], cxl_test was updated to register mock memory-devices after the mock root-port/bus device had been registered. That led to cxl_test crashing with a use-after-free bug with the following signature: cxl_port_attach_region: cxl region3: cxl_host_bridge.0:port3 decoder3.0 add: mem0:decoder7.0 @ 0 next: cxl_switch_uport.0 nr_eps: 1 nr_targets: 1 cxl_port_attach_region: cxl region3: cxl_host_bridge.0:port3 decoder3.0 add: mem4:decoder14.0 @ 1 next: cxl_switch_uport.0 nr_eps: 2 nr_targets: 1 cxl_port_setup_targets: cxl region3: cxl_switch_uport.0:port6 target[0] = cxl_switch_dport.0 for mem0:decoder7.0 @ 0 1) cxl_port_setup_targets: cxl region3: cxl_switch_uport.0:port6 target[1] = cxl_switch_dport.4 for mem4:decoder14.0 @ 1 [..] cxld_unregister: cxl decoder14.0: cxl_region_decode_reset: cxl_region region3: mock_decoder_reset: cxl_port port3: decoder3.0 reset 2) mock_decoder_reset: cxl_port port3: decoder3.0: out of order reset, expected decoder3.1 cxl_endpoint_decoder_release: cxl decoder14.0: [..] cxld_unregister: cxl decoder7.0: 3) cxl_region_decode_reset: cxl_region region3: Oops: general protection fault, probably for non-canonical address 0x6b6b6b6b6b6b6bc3: 0000 [#1] PREEMPT SMP PTI [..] RIP: 0010:to_cxl_port+0x8/0x60 [cxl_core] [..] Call Trace: <TASK> cxl_region_decode_reset+0x69/0x190 [cxl_core] cxl_region_detach+0xe8/0x210 [cxl_core] cxl_decoder_kill_region+0x27/0x40 [cxl_core] cxld_unregister+0x5d/0x60 [cxl_core] At 1) a region has been established with 2 endpoint decoders (7.0 and 14.0). Those endpoints share a common switch-decoder in the topology (3.0). At teardown, 2), decoder14.0 is the first to be removed and hits the "out of order reset case" in the switch decoder. The effect though is that region3 cleanup is aborted leaving it in-tact and referencing decoder14.0. At 3) the second attempt to teardown region3 trips over the stale decoder14.0 object which has long since been deleted. The fix here is to recognize that the CXL specification places no mandate on in-order shutdown of switch-decoders, the driver enforces in-order allocation, and hardware enforces in-order commit. So, rather than fail and leave objects dangling, always remove them. In support of making cxl_region_decode_reset() always succeed, cxl_region_invalidate_memregion() failures are turned into warnings. Crashing the kernel is ok there since system integrity is at risk if caches cannot be managed around physical address mutation events like CXL region destruction. A new device_for_each_child_reverse_from() is added to cleanup port->commit_end after all dependent decoders have been disabled. In other words if decoders are allocated 0->1->2 and disabled 1->2->0 then port->commit_end only decrements from 2 after 2 has been disabled, and it decrements all the way to zero since 1 was disabled previously.	7.8	More Details
CVE-2024-47442	After Effects versions 23.6.9, 24.6.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-47443	After Effects versions 23.6.9, 24.6.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-47450	Illustrator versions 28.7.1 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-49027	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-49029	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-47452	Illustrator versions 28.7.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-49030	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50246	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: Add rough attr alloc_size check	7.8	More Details
CVE-2024-49051	Microsoft PC Manager Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-50261	In the Linux kernel, the following vulnerability has been resolved: macsec: Fix use-after-free while sending the offloading packet KASAN reports the following UAF. The metadata_dst, which is used to store the SCI value for macsec offload, is already freed by metadata_dst_free() in macsec_free_netdev(), while driver still use it for sending the packet. To fix this issue, dst_release() is used instead to release metadata_dst. So it is not freed instantly in macsec_free_netdev() if still referenced by skb. BUG: KASAN: slab-use-after-free in mlx5e_xmit+0x1e8f/0x4190 [mlx5_core] Read of size 2 at addr ffff88813e42e038 by task kworker/7:2/714 [...] Workqueue: mld mld_ifc_work Call Trace: <TASK> dump_stack_lvl+0x51/0x60 print_report+0xc1/0x600 kasan_report+0xab/0xe0 mlx5e_xmit+0x1e8f/0x4190 [mlx5_core] dev_hard_start_xmit+0x120/0x530 sch_direct_xmit+0x149/0x11e0 __qdisc_run+0x3ad/0x1730 __dev_queue_xmit+0x1196/0x2ed0 vlan_dev_hard_start_xmit+0x32e/0x510 [8021q] dev_hard_start_xmit+0x120/0x530 __dev_queue_xmit+0x14a7/0x2ed0 macsec_start_xmit+0x13e9/0x2340 dev_hard_start_xmit+0x120/0x530 __dev_queue_xmit+0x14a7/0x2ed0 ip6_finish_output2+0x923/0x1a70 ip6_finish_output+0x2d7/0x970 ip6_output+0x1ce/0x3a0 NF_HOOK.constprop.0+0x15f/0x190 mld_sendpack+0x59a/0xbd0 mld_ifc_work+0x48a/0xa80 process_one_work+0x5aa/0xe50 worker_thread+0x79c/0x1290 kthread+0x28f/0x350 ret_from_fork+0x2d/0x70 ret_from_fork_asm+0x11/0x20 </TASK> Allocated by task 3922: kasan_save_stack+0x20/0x40 kasan_save_track+0x10/0x30 __kasan_kmalloc+0x77/0x90 __kmalloc_noprof+0x188/0x400 metadata_dst_alloc+0x1f/0x4e0 macsec_newlink+0x914/0x1410 __rtnl_newlink+0xe08/0x15b0 rtnl_newlink+0x5f/0x90 rtnetlink_rcv_msg+0x667/0xa80 netlink_rcv_skb+0x12c/0x360 netlink_unicast+0x551/0x770 netlink_sendmsg+0x72d/0xbd0 __sock_sendmsg+0xc5/0x190 ____sys_sendmsg+0x52e/0x6a0 ___sys_sendmsg+0xeb/0x170 __sys_sendmsg+0xb5/0x140 do_syscall_64+0x4c/0x100 entry_SYSCALL_64_after_hwframe+0x4b/0x53 Freed by task 4011: kasan_save_stack+0x20/0x40 kasan_save_track+0x10/0x30 kasan_save_free_info+0x37/0x50 poison_slab_object+0x10c/0x190 __kasan_slab_free+0x11/0x30 kfree+0xe0/0x290 macsec_free_netdev+0x3f/0x140 netdev_run_todo+0x450/0xc70 rtnetlink_rcv_msg+0x66f/0xa80 netlink_rcv_skb+0x12c/0x360 netlink_unicast+0x551/0x770 netlink_sendmsg+0x72d/0xbd0 __sock_sendmsg+0xc5/0x190 ____sys_sendmsg+0x52e/0x6a0 ___sys_sendmsg+0xeb/0x170 __sys_sendmsg+0xb5/0x140 do_syscall_64+0x4c/0x100 entry_SYSCALL_64_after_hwframe+0x4b/0x53	7.8	More Details
CVE-2024-49557	Dell SmartFabric OS10 Software, version(s) 10.5.6.x, 10.5.5.x, 10.5.4.x, 10.5.3.x, contain(s) an Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution.	7.8	More Details
CVE-2024-49046	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-50262	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix out-of-bounds write in trie_get_next_key() trie_get_next_key() allocates a node stack with size trie->max_prefixlen, while it writes (trie->max_prefixlen + 1) nodes to the stack when it has full paths from the root to leaves. For example, consider a trie with max_prefixlen is 8, and the nodes with key 0x00/0, 0x00/1, 0x00/2, ... 0x00/8 inserted. Subsequent calls to trie_get_next_key with _key with .prefixlen = 8 make 9 nodes be written on the node stack with size 8.	7.8	More Details
CVE-2024-49558	Dell SmartFabric OS10 Software, version(s) 10.5.6.x, 10.5.5.x, 10.5.4.x, 10.5.3.x, contain(s) an Improper Privilege Management vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	7.8	More Details
CVE-2024-49043	Microsoft.SqlServer.XEvent.Configuration.dll Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49560	Dell SmartFabric OS10 Software, version(s) 10.5.6.x, 10.5.5.x, 10.5.4.x, 10.5.3.x, contain(s) a command injection vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Command execution.	7.8	More Details
CVE-2024-50242	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: Additional check in ntfs_file_release	7.8	More Details
CVE-2024-50235	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: clear wdev->cqm_config pointer on free When we free wdev->cqm_config when unregistering, we also need to clear out the pointer since the same wdev/netdev may get re-registered in another network namespace, then destroyed later, running this code again, which results in a double-free.	7.8	More Details
CVE-2024-29119	A vulnerability has been identified in Spectrum Power 7 (All versions < V24Q3). The affected product contains several root-owned SUID binaries that could allow an authenticated local attacker to escalate privileges.	7.8	More Details
CVE-2024-49032	Microsoft Office Graphics Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-49031	Microsoft Office Graphics Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-50143	In the Linux kernel, the following vulnerability has been resolved: udf: fix uninit-value use in udf_get_fileshortad Check for overflow when computing alen in udf_current_aext to mitigate later uninit-value use in udf_get_fileshortad KMSAN bug[1]. After applying the patch reproducer did not trigger any issue[2]. [1] https://syzkaller.appspot.com/bug?extid=8901c4560b7ab5c2f9df [2] https://syzkaller.appspot.com/x/log.txt?x=10242227980000	7.8	More Details
CVE-2024-49515	Substance3D - Painter versions 10.1.0 and earlier are affected by an Untrusted Search Path vulnerability that might allow attackers to execute arbitrary code. If the application uses a search path to locate critical resources such as programs, then an attacker could modify that search path to point to a malicious program, which the targeted application would then execute. The problem extends to any type of critical resource that the application trusts. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-47451	Illustrator versions 28.7.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-50217	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix use-after-free of block device file in __btrfs_free_extra_devids() Mounting btrfs from two images (which have the same one fsid and two different dev_uuids) in certain executing order may trigger an UAF for variable 'device->bdev_file' in __btrfs_free_extra_devids(). And following are the details: 1. Attach image_1 to loop0, attach image_2 to loop1, and scan btrfs devices by ioctl(BTRFS_IOC_SCAN_DEV): / btrfs_device_1 → loop0 fs_device \ btrfs_device_2 → loop1 2. mount /dev/loop0 /mnt btrfs_open_devices btrfs_device_1->bdev_file = btrfs_get_bdev_and_sb(loop0) btrfs_device_2->bdev_file = btrfs_get_bdev_and_sb(loop1) btrfs_fill_super open_ctree fail: btrfs_close_devices // -ENOMEM btrfs_close_bdev(btrfs_device_1) fput(btrfs_device_1->bdev_file) // btrfs_device_1->bdev_file is freed btrfs_close_bdev(btrfs_device_2) fput(btrfs_device_2->bdev_file) 3. mount /dev/loop1 /mnt btrfs_open_devices btrfs_get_bdev_and_sb(&bdev_file) // EIO, btrfs_device_1->bdev_file is not assigned, // which points to a freed memory area btrfs_device_2->bdev_file = btrfs_get_bdev_and_sb(loop1) btrfs_fill_super open_ctree btrfs_free_extra_devids if (btrfs_device_1->bdev_file) fput(btrfs_device_1->bdev_file) // UAF ! Fix it by setting 'device->bdev_file' as 'NULL' after closing the btrfs_device in btrfs_close_one_device().	7.8	More Details
CVE-2024-47426	Substance3D - Painter versions 10.1.0 and earlier are affected by a Double Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47434	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-47433	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-47432	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-47431	Substance3D - Painter versions 10.1.0 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-46954	An issue was discovered in decode_utf8 in base/gp_utf8.c in Artifex Ghostscript before 10.04.0. Overlong UTF-8 encoding leads to possible ../ directory traversal.	7.8	More Details
CVE-2024-47430	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-47429	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-47428	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-50215	In the Linux kernel, the following vulnerability has been resolved: nvmet-auth: assign dh_key to NULL after kfree_sensitive ctrl->dh_key might be used across multiple calls to nvmet_setup_dhgroup() for the same controller. So it's better to nullify it after release on error path in order to avoid double free later in nvmet_destroy_auth(). Found by Linux Verification Center (linuxtesting.org) with Svace.	7.8	More Details
CVE-2024-46953	An issue was discovered in base/gsdevice.c in Artifex Ghostscript before 10.04.0. An integer overflow when parsing the filename format string (for the output filename) results in path truncation, and possible path traversal and code execution.	7.8	More Details
CVE-2024-47427	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-46952	An issue was discovered in pdf/pdf_xref.c in Artifex Ghostscript before 10.04.0. There is a buffer overflow during handling of a PDF XRef stream (related to W array values).	7.8	More Details
CVE-2024-39605	If an attacker tricks a valid user into running Delta Electronics DIAScreen with a file containing malicious code, a stack-based buffer overflow in BACnetParameter can be exploited, allowing the attacker to remotely execute arbitrary code.	7.8	More Details
CVE-2024-47940	A vulnerability has been identified in Solid Edge SE2024 (All versions < V224.0 Update 9). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PSM files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-47941	A vulnerability has been identified in Solid Edge SE2024 (All versions < V224.0 Update 9). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47783	A vulnerability has been identified in SIPORT (All versions < V3.4.0). The affected application improperly assigns file permissions to installation folders. This could allow a local attacker with an unprivileged account to override or modify the service executables and subsequently gain elevated privileges.	7.8	More Details
CVE-2024-46951	An issue was discovered in psi/zcolor.c in Artifex Ghostscript before 10.04.0. An unchecked Implementation pointer in Pattern color space could lead to arbitrary code execution.	7.8	More Details
CVE-2024-50222	In the Linux kernel, the following vulnerability has been resolved: iov_iter: fix copy_page_from_iter_atomic() if KMAP_LOCAL_FORCE_MAP generic/077 on x86_32 CONFIG_DEBUG_KMAP_LOCAL_FORCE_MAP=y with highmem, on huge=always tmpfs, issues a warning and then hangs (interruptibly): WARNING: CPU: 5 PID: 3517 at mm/highmem.c:622 kunmap_local_indexed+0x62/0xc9 CPU: 5 UID: 0 PID: 3517 Comm: cp Not tainted 6.12.0-rc4 #2 ... copy_page_from_iter_atomic+0xa6/0x5ec generic_perform_write+0xf6/0x1b4 shmem_file_write_iter+0x54/0x67 Fix copy_page_from_iter_atomic() by limiting it in that case (include/linux/skbuff.h skb_frag_must_loop() does similar). But going forward, perhaps CONFIG_DEBUG_KMAP_LOCAL_FORCE_MAP is too surprising, has outlived its usefulness, and should just be removed?	7.8	More Details
CVE-2024-50221	In the Linux kernel, the following vulnerability has been resolved: drm/amd/pm: Vangogh: Fix kernel memory out of bounds write KASAN reports that the GPU metrics table allocated in vangogh_tables_init() is not large enough for the memset done in smu_cmn_init_soft_gpu_metrics(). Condensed report follows: [33.861314] BUG: KASAN: slab-out-of-bounds in smu_cmn_init_soft_gpu_metrics+0x73/0x200 [amdgpu] [33.861799] Write of size 168 at addr ffff888129f59500 by task mangoapp/1067 ... [33.861808] CPU: 6 UID: 1000 PID: 1067 Comm: mangoapp Tainted: G W 6.12.0-rc4 #356 1a56f59a8b5182eeaf67eb7cb8b13594dd23b544 [33.861816] Tainted: [W]=WARN [33.861818] Hardware name: Valve Galileo/Galileo, BIOS F7G0107 12/01/2023 [33.861822] Call Trace: [33.861826] <TASK> [33.861829] dump_stack_lvl+0x66/0x90 [33.861838] print_report+0xce/0x620 [33.861853] kasan_report+0xda/0x110 [33.862794] kasan_check_range+0xfd/0x1a0 [33.862799] __asan_memset+0x23/0x40 [33.862803] smu_cmn_init_soft_gpu_metrics+0x73/0x200 [amdgpu 13b1bc364ec578808f676eba412c20eaab792779] [33.863306] vangogh_get_gpu_metrics_v2_4+0x123/0xad0 [amdgpu 13b1bc364ec578808f676eba412c20eaab792779] [33.864257] vangogh_common_get_gpu_metrics+0xb0c/0xbc0 [amdgpu 13b1bc364ec578808f676eba412c20eaab792779] [33.865682] amdgpu_dpm_get_gpu_metrics+0xcc/0x110 [amdgpu 13b1bc364ec578808f676eba412c20eaab792779] [33.866160] amdgpu_get_gpu_metrics+0x154/0x2d0 [amdgpu 13b1bc364ec578808f676eba412c20eaab792779] [33.867135] dev_attr_show+0x43/0xc0 [33.867147] sysfs_kf_seq_show+0x1f1/0x3b0 [33.867155] seq_read_iter+0x3f8/0x1140 [33.867173] vfs_read+0x76c/0xc50 [33.867198] ksys_read+0xfb/0x1d0 [33.867214] do_syscall_64+0x90/0x160 ... [33.867353] Allocated by task 378 on cpu 7 at 22.794876s: [33.867358] kasan_save_stack+0x33/0x50 [33.867364] kasan_save_track+0x17/0x60 [33.867367] __kasan_kmalloc+0x87/0x90 [33.867371] vangogh_init_smc_tables+0x3f9/0x840 [amdgpu] [33.867835] smu_sw_init+0xa32/0x1850 [amdgpu] [33.868299] amdgpu_device_init+0x467b/0x8d90 [amdgpu] [33.868733] amdgpu_driver_load_kms+0x19/0xf0 [amdgpu] [33.869167] amdgpu_pci_probe+0x2d6/0xcd0 [amdgpu] [33.869608] local_pci_probe+0xda/0x180 [33.869614] pci_device_probe+0x43f/0x6b0 Empirically we can confirm that the former allocates 152 bytes for the table, while the latter memsets the 168 large block. Root cause appears that when GPU metrics tables for v2_4 parts were added it was not considered to enlarge the table to fit. The fix in this patch is rather "brute force" and perhaps later should be done in a smarter way, by extracting and consolidating the part version to size logic to a common helper, instead of brute forcing the largest possible allocation. Nevertheless, for now this works and fixes the out of bounds write. v2: * Drop impossible v3_0 case. (Mario) (cherry picked from commit 0880f58f9609f0200483a49429af0f050d281703)	7.8	More Details
CVE-2024-43428	To address a cache poisoning risk in Moodle, additional validation for local storage was required.	7.7	More Details
CVE-2024-49521	Adobe Commerce versions 3.2.5 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to a security feature bypass. A low privileged attacker could exploit this vulnerability to send crafted requests from the vulnerable server to internal systems, which could result in the bypassing of security measures such as firewalls. Exploitation of this issue does not require user interaction.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10975	Nomad Community and Nomad Enterprise ("Nomad") volume specification is vulnerable to arbitrary cross-namespace volume creation through unauthorized Container Storage Interface (CSI) volume writes. This vulnerability, identified as CVE-2024-10975, is fixed in Nomad Community Edition 1.9.2 and Nomad Enterprise 1.9.2, 1.8.7, and 1.7.15.	7.7	More Details
CVE-2021-27700	SOCIFI Socifi Guest wifi as SAAS wifi portal is affected by Insecure Permissions. Any authorized customer with partner mode can switch to another customer dashboard and perform actions like modify user, delete user, etc.	7.6	More Details
CVE-2020-11859	Improper Input Validation vulnerability in OpenText iManager allows Cross-Site Scripting (XSS). This issue affects iManager before 3.2.3	7.6	More Details
CVE-2024-45289	The fetch(3) library uses environment variables for passing certain information, including the revocation file pathname. The environment variable name used by fetch(1) to pass the filename to the library was incorrect, in effect ignoring the option. Fetch would still connect to a host presenting a certificate included in the revocation file passed to the --crl option.	7.5	More Details
CVE-2024-52530	GNOME libsoup before 3.6.0 allows HTTP request smuggling in some configurations because '\0' characters at the end of header names are ignored, i.e., a "Transfer-Encoding\0: chunked" header is treated the same as a "Transfer-Encoding: chunked" header.	7.5	More Details
CVE-2024-48939	Insufficient validation performed on the REST API License file in Paxton Net2 before 6.07.14023.5015 (SR4) enables use of the REST API with an invalid License File. Attackers may be able to retrieve access-log data.	7.5	More Details
CVE-2024-27532	wasm-micro-runtime (aka WebAssembly Micro Runtime or WAMR) 06df58f is vulnerable to NULL Pointer Dereference in function `block_type_get_result_types.	7.5	More Details
CVE-2024-50331	An out-of-bounds read vulnerability in Ivanti Avalanche before 6.4.6 allows a remote unauthenticated attacker to leak sensitive information in memory.	7.5	More Details
CVE-2024-50589	An unauthenticated attacker with access to the local network of the medical office can query an unprotected Fast Healthcare Interoperability Resources (FHIR) API to get access to sensitive electronic health records (EHR).	7.5	More Details
CVE-2024-27527	wasm3 139076a is vulnerable to Denial of Service (DoS).	7.5	More Details
CVE-2024-11067	The D-Link DSL6740C modem has a Path Traversal Vulnerability, allowing unauthenticated remote attackers to exploit this vulnerability to read arbitrary system files. Additionally, since the device's default password is a combination of the MAC address, attackers can obtain the MAC address through this vulnerability and attempt to log in to the device using the default password.	7.5	More Details
CVE-2024-50320	An infinite loop in Ivanti Avalanche before 6.4.6 allows a remote unauthenticated attacker to cause a denial of service.	7.5	More Details
CVE-2021-41737	In Faust 2.23.1, an input file with the lines "// r visualisation tCst" and "//process = +: L: abM-^Q;" and "process = route(3333333333333333333,2,1,2,3,1) : *;" leads to stack consumption.	7.5	More Details
CVE-2024-51564	A guest can trigger an infinite loop in the hda audio driver.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50319	An infinite loop in Ivanti Avalanche before 6.4.6 allows a remote unauthenticated attacker to cause a denial of service.	7.5	More Details
CVE-2024-47907	A stack-based buffer overflow in IPsec of Ivanti Connect Secure before version 22.7R2.3 allows a remote unauthenticated attacker to cause a denial of service.	7.5	More Details
CVE-2024-8495	A null pointer dereference in Ivanti Connect Secure before version 22.7R2.1 and Ivanti Policy Secure before version 22.7R1.1 allows a remote unauthenticated attacker to cause a denial of service.	7.5	More Details
CVE-2024-50317	A null pointer dereference in Ivanti Avalanche before 6.4.6 allows a remote unauthenticated attacker to cause a denial of service.	7.5	More Details
CVE-2024-50318	A null pointer dereference in Ivanti Avalanche before 6.4.6 allows a remote unauthenticated attacker to cause a denial of service.	7.5	More Details
CVE-2024-50310	A vulnerability has been identified in SIMATIC CP 1543-1 V4.0 (6GK7543-1AX10-0XE0) (All versions >= V4.0.44 < V4.0.50). Affected devices do not properly handle authorization. This could allow an unauthenticated remote attacker to gain access to the filesystem.	7.5	More Details
CVE-2024-50321	An infinite loop in Ivanti Avalanche before 6.4.6 allows a remote unauthenticated attacker to cause a denial of service.	7.5	More Details
CVE-2024-25253	Driver Booster v10.6 was discovered to contain a buffer overflow via the Host parameter under the Customize proxy module.	7.5	More Details
CVE-2024-52532	GNOME libsoup before 3.6.1 has an infinite loop, and memory consumption. during the reading of certain patterns of WebSocket data from clients.	7.5	More Details
CVE-2024-10028	The Everest Backup – WordPress Cloud Backup, Migration, Restore & Cloning Plugin plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.2.13 via the exposed process stats file during the backup process. This makes it possible for unauthenticated attackers to obtain an archive file name and download the site's backup.	7.5	More Details
CVE-2024-23666	A client-side enforcement of server-side security in Fortinet FortiAnalyzer-BigData at least version 7.4.0 and 7.2.0 through 7.2.6 and 7.0.1 through 7.0.6 and 6.4.5 through 6.4.7 and 6.2.5, FortiManager version 7.4.0 through 7.4.1 and 7.2.0 through 7.2.4 and 7.0.0 through 7.0.11 and 6.4.0 through 6.4.14, FortiAnalyzer version 7.4.0 through 7.4.1 and 7.2.0 through 7.2.4 and 7.0.0 through 7.0.11 and 6.4.0 through 6.4.14 allows attacker to improper access control via crafted requests.	7.5	More Details
CVE-2024-43499	.NET and Visual Studio Denial of Service Vulnerability	7.5	More Details
CVE-2024-43450	Windows DNS Spoofing Vulnerability	7.5	More Details
CVE-2024-49033	Microsoft Word Security Feature Bypass Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43426	A flaw was found in pdfTeX. Insufficient sanitizing in the TeX notation filter resulted in an arbitrary file read risk on sites where pdfTeX is available, such as those with TeX Live installed.	7.5	More Details
CVE-2024-43431	A vulnerability was found in Moodle. Insufficient capability checks made it possible to delete badges that a user does not have permission to access.	7.5	More Details
CVE-2024-43438	A flaw was found in Feedback. Bulk messaging in the activity's non-respondents report did not verify message recipients belonging to the set of users returned by the report.	7.5	More Details
CVE-2024-43452	Windows Registry Elevation of Privilege Vulnerability	7.5	More Details
CVE-2024-43440	A flaw was found in moodle. A local file may include risks when restoring block backups.	7.5	More Details
CVE-2024-48950	An issue was discovered in Logpoint before 7.5.0. An endpoint used by Distributed Logpoint Setup was exposed, allowing unauthenticated attackers to bypass CSRF protections and authentication.	7.5	More Details
CVE-2024-49040	Microsoft Exchange Server Spoofing Vulnerability	7.5	More Details
CVE-2024-48951	An issue was discovered in Logpoint before 7.5.0. Server-Side Request Forgery (SSRF) on SOAR can be used to leak Logpoint's API Token leading to authentication bypass.	7.5	More Details
CVE-2024-48953	An issue was discovered in Logpoint before 7.5.0. Endpoints for creating, editing, or deleting third-party authentication modules lacked proper authorization checks. This allowed unauthenticated users to register their own authentication plugins in Logpoint, resulting in unauthorized access.	7.5	More Details
CVE-2020-11926	An issue was discovered in Luvion Grand Elite 3 Connect through 2020-02-25. Clients can authenticate themselves to the device using a username and password. These credentials can be obtained through an unauthenticated web request, e.g., for a JavaScript file. Also, the disclosed information includes the SSID and WPA2 key for the Wi-Fi network the device is connected to.	7.5	More Details
CVE-2024-21538	Versions of the package cross-spawn before 7.0.5 are vulnerable to Regular Expression Denial of Service (ReDoS) due to improper input sanitization. An attacker can increase the CPU usage and crash the program by crafting a very large and well crafted string.	7.5	More Details
CVE-2024-51428	An issue in Espressif Esp idf v5.3.0 allows attackers to cause a Denial of Service (DoS) via a crafted data channel packet.	7.5	More Details
CVE-2024-43642	Windows SMB Denial of Service Vulnerability	7.5	More Details
CVE-2024-36063	The Goodwy com.goodwy.dialer (aka Right Dialer) application through 5.1.0 for Android enables any application (with no permissions) to place phone calls without user interaction by sending a crafted intent via the com.goodwy.dialer.activities.DialerActivity component.	7.5	More Details
CVE-2023-1973	A flaw was found in Undertow package. Using the FormAuthenticationMechanism, a malicious user could trigger a Denial of Service by sending crafted requests, leading the server to an OutofMemory error, exhausting the server's memory.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47072	XStream is a simple library to serialize objects to XML and back again. This vulnerability may allow a remote attacker to terminate the application with a stack overflow error resulting in a denial of service only by manipulating the processed input stream when XStream is configured to use the BinaryStreamDriver. XStream 1.4.21 has been patched to detect the manipulation in the binary input stream causing the the stack overflow and raises an InputManipulationException instead. Users are advised to upgrade. Users unable to upgrade may catch the StackOverflowError in the client code calling XStream if XStream is configured to use the BinaryStreamDriver.	7.5	More Details
CVE-2024-51179	An issue in Open 5GS v.2.7.1 allows a remote attacker to cause a denial of service via the Network Function Virtualizations (NFVs) such as the User Plane Function (UPF) and the Session Management Function (SMF), The Packet Data Unit (PDU) session establishment process.	7.5	More Details
CVE-2023-50176	A session fixation in Fortinet FortiOS version 7.4.0 through 7.4.3 and 7.2.0 through 7.2.7 and 7.0.0 through 7.0.13 allows attacker to execute unauthorized code or commands via phishing SAML authentication link.	7.5	More Details
CVE-2024-6861	A disclosure of sensitive information flaw was found in foreman via the GraphQL API. If the introspection feature is enabled, it is possible for attackers to retrieve sensitive admin authentication keys which could result in a compromise of the entire product's API.	7.5	More Details
CVE-2024-40592	An improper verification of cryptographic signature vulnerability [CWE-347] in FortiClient MacOS version 7.4.0, version 7.2.4 and below, version 7.0.10 and below, version 6.4.10 and below may allow a local authenticated attacker to swap the installer with a malicious package via a race condition during the installation process.	7.5	More Details
CVE-2024-20484	A vulnerability in the External Agent Assignment Service (EAAS) feature of Cisco Enterprise Chat and Email (ECE) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of Media Routing Peripheral Interface Manager (MR PIM) traffic that is received by an affected device. An attacker could exploit this vulnerability by sending crafted MR PIM traffic to an affected device. A successful exploit could allow the attacker to trigger a failure on the MR PIM connection between Cisco ECE and Cisco Unified Contact Center Enterprise (CCE), leading to a DoS condition on EAAS that would prevent customers from starting chat, callback, or delayed callback sessions. Note: When the attack traffic stops, the EAAS process must be manually restarted to restore normal operation. To restart the process in the System Console, choose Shared Resources > Services > Unified CCE > EAAS, then click Start.	7.5	More Details
CVE-2024-10963	A flaw was found in pam_access, where certain rules in its configuration file are mistakenly treated as hostnames. This vulnerability allows attackers to trick the system by pretending to be a trusted hostname, gaining unauthorized access. This issue poses a risk for systems that rely on this feature to control who can access certain services or terminals.	7.4	More Details
CVE-2024-49393	In neomutt and mutt, the To and Cc email headers are not validated by cryptographic signing which allows an attacker that intercepts a message to change their value and include himself as a one of the recipients to compromise message confidentiality.	7.4	More Details
CVE-2024-37365	A remote code execution vulnerability exists in the affected product. The vulnerability allows users to save projects within the public directory allowing anyone with local access to modify and/or delete files. Additionally, a malicious user could potentially leverage this vulnerability to escalate their privileges by changing the macro to execute arbitrary code.	7.3	More Details
CVE-2021-27702	Sercomm Router Etisalat Model S3- AC2100 is affected by Incorrect Access Control via the diagnostic utility in the router dashboard.	7.3	More Details
CVE-2024-10969	A vulnerability was found in 1000 Projects Bookstore Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/login_process.php of the component Login. The manipulation of the argument unm 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 Number	Description	Base Score	Reference
CVE-2024-10968	A vulnerability was found in 1000 Projects Bookstore Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /contact_process.php. The manipulation of the argument fnm 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-2024-11077	A vulnerability, which was classified as critical, was found in code-projects Job Recruitment 1.0. Affected is an unknown function of the file /index.php. The manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-10967	A vulnerability was found in code-projects E-Health Care System 1.0. It has been classified as critical. Affected is an unknown function of the file /Doctor/delete_user_appointment_request.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.	7.3	More Details
CVE-2024-11057	A vulnerability has been found in Codezips Hospital Appointment System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /removeBranchResult.php. The manipulation of the argument ID/Name 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-2024-11055	A vulnerability, which was classified as critical, has been found in 1000 Projects Beauty Parlour Management System 1.0. This issue affects some unknown processing of the file /admin/admin-profile.php. The manipulation of the argument adminname 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-2024-11100	A vulnerability was found in 1000 Projects Beauty Parlour Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /index.php. The manipulation of the argument name 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-2024-10958	The The WP Photo Album Plus plugin for WordPress is vulnerable to arbitrary shortcode execution via getshortcodedrenderedfenodelay AJAX action in all versions up to, and including, 8.8.08.007 . This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	7.3	More Details
CVE-2024-49056	Authentication bypass by assumed-immutable data on airlift.microsoft.com allows an authorized attacker to elevate privileges over a network.	7.3	More Details
CVE-2024-47942	A vulnerability has been identified in Solid Edge SE2024 (All versions < V224.0 Update 9). The affected applications suffer from a DLL hijacking vulnerability. This could allow an attacker to execute arbitrary code via placing a crafted DLL file on the system.	7.3	More Details
CVE-2024-51721	A code injection vulnerability in the SecuSUITE Server Web Administration Portal of SecuSUITE versions 5.0.420 and earlier could allow an attacker to potentially inject script commands or other executable content into the server that would run with root privilege.	7.3	More Details
CVE-2024-50340	symfony/runtime is a module for the Symphony PHP framework which enables decoupling PHP applications from global state. When the `register_argv_argc` php directive is set to `on` , and users call any URL with a special crafted query string, they are able to change the environment or debug mode used by the kernel when handling the request. As of versions 5.4.46, 6.4.14, and 7.1.7 the `SymfonyRuntime` now ignores the `argv` values for non-SAPI PHP runtimes. All users are advised to upgrade. There are no known workarounds for this vulnerability.	7.3	More Details
CVE-2024-36507	A untrusted search path in Fortinet FortiClientWindows versions 7.4.0, versions 7.2.4 through 7.2.0, versions 7.0.12 through 7.0.0 allows an attacker to run arbitrary code via DLL hijacking and social engineering.	7.3	More Details
CVE-2024-10640	The The FOX – Currency Switcher Professional for WooCommerce plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 1.4.2.2. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10261	The The Paid Membership Subscriptions – Effortless Memberships, Recurring Payments & Content Restriction plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 2.13.0. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	7.3	More Details
CVE-2024-10996	A vulnerability was found in 1000 Projects Bookstore Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/process_category_edit.php. The manipulation of the argument cat leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-10988	A vulnerability was found in code-projects E-Health Care System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /Doctor/doctor_login.php. The manipulation of the argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	7.3	More Details
CVE-2024-11099	A vulnerability was found in code-projects Job Recruitment 1.0 and classified as critical. This issue affects some unknown processing of the file /login.php. The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2023-32736	A vulnerability has been identified in SIMATIC S7-PLCSIM V16 (All versions), SIMATIC S7-PLCSIM V17 (All versions), SIMATIC STEP 7 Safety V16 (All versions), SIMATIC STEP 7 Safety V17 (All versions < V17 Update 8), SIMATIC STEP 7 Safety V18 (All versions < V18 Update 5), SIMATIC STEP 7 V16 (All versions), SIMATIC STEP 7 V17 (All versions < V17 Update 8), SIMATIC STEP 7 V18 (All versions < V18 Update 5), SIMATIC WinCC Unified V16 (All versions), SIMATIC WinCC Unified V17 (All versions < V17 Update 8), SIMATIC WinCC Unified V18 (All versions < V18 Update 5), SIMATIC WinCC V16 (All versions), SIMATIC WinCC V17 (All versions < V17 Update 8), SIMATIC WinCC V18 (All versions < V18 Update 5), SIMOCODE ES V16 (All versions), SIMOCODE ES V17 (All versions < V17 Update 8), SIMOCODE ES V18 (All versions), SIMOTION SCOUT TIA V5.4 SP1 (All versions), SIMOTION SCOUT TIA V5.4 SP3 (All versions), SIMOTION SCOUT TIA V5.5 SP1 (All versions), SINAMICS Startdrive V16 (All versions), SINAMICS Startdrive V17 (All versions), SINAMICS Startdrive V18 (All versions), SIRIUS Safety ES V17 (All versions < V17 Update 8), SIRIUS Safety ES V18 (All versions), SIRIUS Soft Starter ES V17 (All versions < V17 Update 8), SIRIUS Soft Starter ES V18 (All versions), TIA Portal Cloud V16 (All versions), TIA Portal Cloud V17 (All versions < V4.6.0.1), TIA Portal Cloud V18 (All versions < V4.6.1.0). Affected products do not properly sanitize user-controllable input when parsing user settings. This could allow an attacker to cause a type confusion and execute arbitrary code within the affected application.	7.3	More Details
CVE-2024-10995	A vulnerability was found in Codezips Hospital Appointment System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /removeDoctorResult.php. The manipulation of the argument Name 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-2024-21937	Incorrect default permissions in the AMD HIP SDK installation directory could allow an attacker to achieve privilege escalation potentially resulting in arbitrary code execution.	7.3	More Details
CVE-2024-9842	Incorrect permissions in Ivanti Secure Access Client before version 22.7R4 allows a local authenticated attacker to create arbitrary folders.	7.3	More Details
CVE-2024-21945	Incorrect default permissions in the AMD RyzenTM Master monitoring SDK installation directory could allow an attacker to achieve privilege escalation potentially resulting in arbitrary code execution.	7.3	More Details
CVE-2024-21938	Incorrect default permissions in the AMD Management Plugin for the Microsoft® System Center Configuration Manager (SCCM) installation directory could allow an attacker to achieve privilege escalation, potentially resulting in arbitrary code execution.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21939	Incorrect default permissions in the AMD Cloud Manageability Service (ACMS) Software installation directory could allow an attacker to achieve privilege escalation potentially resulting in arbitrary code execution.	7.3	More Details
CVE-2024-21946	Incorrect default permissions in the AMD RyzenTM Master Utility installation directory could allow an attacker to achieve privilege escalation potentially resulting in arbitrary code execution.	7.3	More Details
CVE-2024-10945	A Local Privilege Escalation vulnerability exists in the affected product. The vulnerability requires a local, low privileged threat actor to replace certain files during update and exists due to a failure to perform proper security checks before installation.	7.3	More Details
CVE-2024-21957	Incorrect default permissions in the AMD Management Console installation directory could allow an attacker to achieve privilege escalation potentially resulting in arbitrary code execution.	7.3	More Details
CVE-2024-10991	A vulnerability, which was classified as critical, has been found in Codezips Hospital Appointment System 1.0. This issue affects some unknown processing of the file /editBranchResult.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-2024-21958	Incorrect default permissions in the AMD Provisioning Console installation directory could allow an attacker to achieve privilege escalation, potentially resulting in arbitrary code execution.	7.3	More Details
CVE-2024-10998	A vulnerability was found in 1000 Projects Bookstore Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/process_category_add.php. The manipulation of the argument cat 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-2024-11065	The D-Link DSL6740C modem has an OS Command Injection vulnerability, allowing remote attackers with administrator privileges to inject and execute arbitrary system commands through a specific functionality provided by SSH and Telnet.	7.2	More Details
CVE-2024-50572	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.2), RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2) (All versions < V8.2), SCALANCE M804PB (6GK5804-0AP00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1AA00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1BA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2) (All versions < V8.2), SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) (All versions < V8.2), SCALANCE M874-2 (6GK5874-2AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 (6GK5874-3AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2) (All versions < V8.2), SCALANCE M876-3 (6GK5876-3AA02-2BA2) (All versions < V8.2), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.2), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.2), SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) (All versions < V8.2), SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) (All versions < V8.2), SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1) (All versions < V8.2), SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1) (All versions < V8.2), SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) (All versions < V8.2), SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1) (All versions < V8.2), SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1) (All versions < V8.2), SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1) (All versions < V8.2), SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) (All versions < V8.2), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.2), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All versions < V8.2), SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2) (All versions < V8.2). Affected devices do not properly sanitize an input field. This could allow an authenticated remote attacker with administrative privileges to inject code or spawn a system root shell.	7.2	More Details
CVE-2024-11066	The D-Link DSL6740C modem has an OS Command Injection vulnerability, allowing remote attackers with administrator privileges to inject and execute arbitrary system commands through the specific web page.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49042	Azure Database for PostgreSQL Flexible Server Extension Elevation of Privilege Vulnerability	7.2	More Details
CVE-2024-50324	Path traversal in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	7.2	More Details
CVE-2024-43436	A SQL injection risk flaw was found in the XMLDB editor tool available to site administrators.	7.2	More Details
CVE-2024-50326	SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	7.2	More Details
CVE-2024-50557	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.2), RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2) (All versions < V8.2), SCALANCE M804PB (6GK5804-0AP00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1AA00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1BA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2) (All versions < V8.2), SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) (All versions < V8.2), SCALANCE M874-2 (6GK5874-2AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 (6GK5874-3AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2) (All versions < V8.2), SCALANCE M876-3 (6GK5876-3AA02-2BA2) (All versions < V8.2), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.2), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.2), SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) (All versions < V8.2), SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) (All versions < V8.2), SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1) (All versions < V8.2), SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1) (All versions < V8.2), SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) (All versions < V8.2), SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1) (All versions < V8.2), SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1) (All versions < V8.2), SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1) (All versions < V8.2), SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) (All versions < V8.2), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.2), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All versions < V8.2), SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2) (All versions < V8.2). Affected devices do not properly validate input in configuration fields of the iperf functionality. This could allow an unauthenticated remote attacker to execute arbitrary code on the device.	7.2	More Details
CVE-2024-51152	File Upload vulnerability in Laravel CMS v.1.4.7 and before allows a remote attacker to execute arbitrary code via the shell.php a component.	7.2	More Details
CVE-2024-50327	SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	7.2	More Details
CVE-2024-42442	APTIOV contains a vulnerability in the BIOS where a user or attacker may cause an improper restriction of operations within the bounds of a memory buffer over the network. A successful exploitation of this vulnerability may lead to code execution outside of the intended System Management Mode.	7.2	More Details
CVE-2024-50328	SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	7.2	More Details
CVE-2024-11062	The D-Link DSL6740C modem has an OS Command Injection vulnerability, allowing remote attackers with administrator privileges to inject and execute arbitrary system commands through a specific functionality provided by SSH and Telnet.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-11063	The D-Link DSL6740C modem has an OS Command Injection vulnerability, allowing remote attackers with administrator privileges to inject and execute arbitrary system commands through a specific functionality provided by SSH and Telnet.	7.2	More Details
CVE-2024-11064	The D-Link DSL6740C modem has an OS Command Injection vulnerability, allowing remote attackers with administrator privileges to inject and execute arbitrary system commands through a specific functionality provided by SSH and Telnet.	7.2	More Details
CVE-2024-43613	Azure Database for PostgreSQL Flexible Server Extension Elevation of Privilege Vulnerability	7.2	More Details
CVE-2024-51689	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Tobias Conrad CF7 WOW Styler allows Reflected XSS.This issue affects CF7 WOW Styler: from n/a through 1.6.8.	7.1	More Details
CVE-2024-51690	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Neelam Samariya Thakor Wp Slide Categorywise allows Reflected XSS.This issue affects Wp Slide Categorywise: from n/a through 1.1.	7.1	More Details
CVE-2024-51676	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Delicious Delisho allows Reflected XSS.This issue affects Delisho: from n/a through 1.0.6.	7.1	More Details
CVE-2024-50193	In the Linux kernel, the following vulnerability has been resolved: x86/entry_32: Clear CPU buffers after register restore in NMI return CPU buffers are currently cleared after call to exc_nmi, but before register state is restored. This may be okay for MDS mitigation but not for RDFS. Because RDFS mitigation requires CPU buffers to be cleared when registers don't have any sensitive data. Move CLEAR_CPU_BUFFERS after RESTORE_ALL_NMI.	7.1	More Details
CVE-2024-51781	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Loop Now Technologies, Inc. Firework Shoppable Live Video allows Reflected XSS.This issue affects Firework Shoppable Live Video: from n/a through 6.3.	7.1	More Details
CVE-2024-51780	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Michael DUMONTET eewee admin custom allows Reflected XSS.This issue affects eewee admin custom: from n/a through 1.8.2.4.	7.1	More Details
CVE-2024-51707	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Webcodin WP Visual Adverts allows Reflected XSS.This issue affects WP Visual Adverts: from n/a through 2.3.0.	7.1	More Details
CVE-2024-50164	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix overloading of MEM_UNINIT's meaning Lonial reported an issue in the BPF verifier where check_mem_size_reg() has the following code: if (!tnum_is_const(reg->var_off)) /* For unprivileged variable accesses, disable raw * mode so that the program is required to * initialize all the memory that the helper could * just partially fill up. */ meta = NULL; This means that writes are not checked when the register containing the size of the passed buffer has not a fixed size. Through this bug, a BPF program can write to a map which is marked as read-only, for example, .rodata global maps. The problem is that MEM_UNINIT's initial meaning that "the passed buffer to the BPF helper does not need to be initialized" which was added back in commit 435faee1aae9 ("bpf, verifier: add ARG_PTR_TO_RAW_STACK type") got overloaded over time with "the passed buffer is being written to". The problem however is that checks such as the above which were added later via 06c1c049721a ("bpf: allow helpers access to variable memory") set meta to NULL in order force the user to always initialize the passed buffer to the helper. Due to the current double meaning of MEM_UNINIT, this bypasses verifier write checks to the memory (not boundary checks though) and only assumes the latter memory is read instead. Fix this by reverting MEM_UNINIT back to its original meaning, and having MEM_WRITE as an annotation to BPF helpers in order to then trigger the BPF verifier checks for writing to memory. Some notes: check_arg_pair_ok() ensures that for ARG_CONST_SIZE{,_OR_ZERO} we can access fn->arg_type[arg - 1] since it must contain a preceding ARG_PTR_TO_MEM. For check_mem_reg() the meta argument can be removed altogether since we do check both BPF_READ and BPF_WRITE. Same for the equivalent check_kfunc_mem_size_reg().	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50227	In the Linux kernel, the following vulnerability has been resolved: thunderbolt: Fix KASAN reported stack out-of-bounds read in tb_retimer_scan() KASAN reported following issue: BUG: KASAN: stack-out-of-bounds in tb_retimer_scan+0xffe/0x1550 [thunderbolt] Read of size 4 at addr ffff88810111fc1c by task kworker/u56:0/11 CPU: 0 UID: 0 PID: 11 Comm: kworker/u56:0 Tainted: G U 6.11.0+ #1387 Tainted: [U]=USER Workqueue: thunderbolt0 tb_handle_hotplug [thunderbolt] Call Trace: <TASK> dump_stack_lvl+0x6c/0x90 print_report+0xd1/0x630 kasan_report+0xdb/0x110 __asan_report_load4_noabort+0x14/0x20 tb_retimer_scan+0xffe/0x1550 [thunderbolt] tb_scan_port+0xa6f/0x2060 [thunderbolt] tb_handle_hotplug+0x17b1/0x3080 [thunderbolt] process_one_work+0x626/0x1100 worker_thread+0x6c8/0xfa0 kthread+0x2c8/0x3a0 ret_from_fork+0x3a/0x80 ret_from_fork_asm+0x1a/0x30 This happens because the loop variable still gets incremented by one so max becomes 3 instead of 2, and this makes the second loop read past the the array declared on the stack. Fix this by assigning to max directly in the loop body.	7.1	More Details
CVE-2024-8539	Improper authorization in Ivanti Secure Access Client before version 22.7R3 allows a local authenticated attacker to modify sensitive configuration files.	7.1	More Details
CVE-2024-51761	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Zack Gilbert and Paul Jarvis WPHelpful allows Reflected XSS.This issue affects WPHelpful: from n/a through 1.2.4.	7.1	More Details
CVE-2024-51716	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Gopi.R Twitter real time search scrolling allows Reflected XSS.This issue affects Twitter real time search scrolling: from n/a through 7.0.	7.1	More Details
CVE-2024-51711	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in saragna Saragna allows Reflected XSS.This issue affects Saragna: from n/a through 1.0.	7.1	More Details
CVE-2024-51712	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Visser Labs Jigoshop – Store Toolkit allows Reflected XSS.This issue affects Jigoshop – Store Toolkit: from n/a through 1.4.0.	7.1	More Details
CVE-2024-51713	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in TRe Technology And Research S.R.L HQ60 Fidelity Card allows Reflected XSS.This issue affects HQ60 Fidelity Card: from n/a through 1.8.	7.1	More Details
CVE-2024-51710	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Minerva Infotech Responsive Data Table allows Reflected XSS.This issue affects Responsive Data Table: from n/a through 1.3.	7.1	More Details
CVE-2024-51714	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Syed Umair Hussain Shah User Password Reset allows Reflected XSS.This issue affects User Password Reset: from n/a through 1.0.	7.1	More Details
CVE-2024-50250	In the Linux kernel, the following vulnerability has been resolved: fsdax: dax_unshare_iter needs to copy entire blocks The code that copies data from srcmap to iomap in dax_unshare_iter is very very broken, which bfoster's recent fsx changes have exposed. If the pos and len passed to dax_file_unshare are not aligned to an fsblock boundary, the iter pos and length in the _iter function will reflect this unalignment. dax_iomap_direct_access always returns a pointer to the start of the kmapped fsdax page, even if its pos argument is in the middle of that page. This is catastrophic for data integrity when iter->pos is not aligned to a page, because daddr/saddr do not point to the same byte in the file as iter->pos. Hence we corrupt user data by copying it to the wrong place. If iter->pos + iomap_length() in the _iter function not aligned to a page, then we fail to copy a full block, and only partially populate the destination block. This is catastrophic for data confidentiality because we expose stale pmem contents. Fix both of these issues by aligning copy_pos/copy_len to a page boundary (remember, this is fsdax so 1 fsblock == 1 base page) so that we always copy full blocks. We're not done yet -- there's no call to invalidate_inode_pages2_range, so programs that have the file range mmap'd will continue accessing the old memory mapping after the file metadata updates have completed. Be careful with the return value -- if the unshare succeeds, we still need to return the number of bytes that the iomap iter thinks we're operating on.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50247	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: Check if more than chunk-size bytes are written A incorrectly formatted chunk may decompress into more than LZNT_CHUNK_SIZE bytes and a index out of bounds will occur in s_max_off.	7.1	More Details
CVE-2024-49049	Visual Studio Code Remote Extension Elevation of Privilege Vulnerability	7.1	More Details
CVE-2024-51760	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in RistrettoApps Dashing Memberships allows Reflected XSS.This issue affects Dashing Memberships: from n/a through 1.1.	7.1	More Details
CVE-2024-51717	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Perception System Ajax Content Filter allows Reflected XSS.This issue affects Ajax Content Filter: from n/a through 1.0.	7.1	More Details
CVE-2024-51718	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Adam Dehnel Simple Modal allows Reflected XSS.This issue affects Simple Modal: from n/a through 0.3.3.	7.1	More Details
CVE-2024-51709	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Marian Dietz TeleAdmin allows Reflected XSS.This issue affects TeleAdmin: from n/a through 1.0.0.	7.1	More Details
CVE-2024-51778	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Starfish Reviews Satisfaction Reports from Help Scout allows Reflected XSS.This issue affects Satisfaction Reports from Help Scout: from n/a through 2.0.3.	7.1	More Details
CVE-2024-51719	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kevin Walker, Roman Peterhans Simplistic SEO allows Reflected XSS.This issue affects Simplistic SEO: from n/a through 2.3.0.	7.1	More Details
CVE-2024-51708	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Narnoo Wordpress developer Narnoo Commerce Manager allows Reflected XSS.This issue affects Narnoo Commerce Manager: from n/a through 1.6.0.	7.1	More Details
CVE-2024-51759	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Detlef Beyer SVT Simple allows Reflected XSS.This issue affects SVT Simple: from n/a through 1.0.1.	7.1	More Details
CVE-2024-51779	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Stranger Studios (WordCamp Philly) Don't Break The Code allows Reflected XSS.This issue affects Don't Break The Code: from n/a through .3.1.	7.1	More Details
CVE-2024-51776	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in samhotchkiss Daily Image allows Reflected XSS.This issue affects Daily Image: from n/a through 1.0.	7.1	More Details
CVE-2024-51698	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Luis Rock Master Bar allows Reflected XSS.This issue affects Master Bar: from n/a through 1.0.	7.1	More Details
CVE-2024-51694	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Digfish Geotagged Media allows Reflected XSS.This issue affects Geotagged Media: from n/a through 0.3.0.	7.1	More Details
CVE-2024-51995	Combodo iTop is a web based IT Service Management tool. An attacker can request any `route` we want as long as we specify an `operation` that is allowed. This issue has been addressed in version 3.2.0 by applying the same access control pattern as in `UI.php` to the `ajax.render.php` page which does not allow arbitrary `routes` to be dispatched. All users are advised to upgrade. There are no known workarounds for this vulnerability.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51994	Combodo iTop is a web based IT Service Management tool. In affected versions uploading a text file containing some java script in the portal will trigger an Cross-site Scripting (XSS) vulnerability. This issue has been addressed in version 3.2.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	7.1	More Details
CVE-2024-51699	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Buooy Buooy Sticky Header allows Reflected XSS.This issue affects Buooy Sticky Header: from n/a through 0.5.2.	7.1	More Details
CVE-2024-51701	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Mahesh Waghmare MG Post Contributors allows Reflected XSS.This issue affects MG Post Contributors: from n/a through 1.3..	7.1	More Details
CVE-2024-51702	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Benjamin Moody, Eric Holmes SrcSet Responsive Images for WordPress allows Reflected XSS.This issue affects SrcSet Responsive Images for WordPress: from n/a through 1.4.	7.1	More Details
CVE-2024-51703	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Genethick WP-Basics allows Reflected XSS.This issue affects WP-Basics: from n/a through 2.0.	7.1	More Details
CVE-2024-51989	Password Pusher is an open source application to communicate sensitive information over the web. A cross-site scripting (XSS) vulnerability was identified in the PasswordPusher application, affecting versions `v1.41.1` through and including `v.1.48.0`. The issue arises from an un-sanitized parameter which could allow attackers to inject malicious JavaScript into the application. Users who self-host and have the login system enabled are affected. Exploitation of this vulnerability could expose user data, access to user sessions or take unintended actions on behalf of users. To exploit this vulnerability, an attacker would need to convince a user to click a malicious account confirmation link. It is highly recommended to update to version `v1.48.1` or later to mitigate this risk. There are no known workarounds for this vulnerability. ### Solution Update to version `v1.48.1` or later where input sanitization has been applied to the account confirmation process. If updating is not immediately possible,	7.1	More Details
CVE-2024-51697	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Doofinder allows Reflected XSS.This issue affects Doofinder: from n/a through 0.5.4.	7.1	More Details
CVE-2024-51704	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Hanusek imPress allows Reflected XSS.This issue affects imPress: from n/a through 0.1.4.	7.1	More Details
CVE-2024-51696	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Benjamin Moody Content Syndication Toolkit Reader allows Reflected XSS.This issue affects Content Syndication Toolkit Reader: from n/a through 1.5.	7.1	More Details
CVE-2024-51695	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Fabrica Fabrica Synced Pattern Instances allows Reflected XSS.This issue affects Fabrica Synced Pattern Instances: from n/a through 1.0.8.	7.1	More Details
CVE-2024-51705	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in James Bruner WP MMenu Lite allows Reflected XSS.This issue affects WP MMenu Lite: from n/a through 1.0.0.	7.1	More Details
CVE-2024-51782	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Sanjaysolutions Loginplus allows Stored XSS.This issue affects Loginplus: from n/a through 1.2.	7.1	More Details
CVE-2024-51706	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Upeksha Wisidagama UW Freelancer allows Reflected XSS.This issue affects UW Freelancer: from n/a through 0.1.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51647	Cross-Site Request Forgery (CSRF) vulnerability in Chaser324 Featured Posts Scroll allows Stored XSS.This issue affects Featured Posts Scroll: from n/a through 1.25.	7.1	More Details
CVE-2024-51783	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in zaus Forms: 3rd-Party Post Again allows Reflected XSS.This issue affects Forms: 3rd-Party Post Again: from n/a through 0.3.	7.1	More Details
CVE-2024-51784	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in VietFriend team FriendStore for WooCommerce allows Reflected XSS.This issue affects FriendStore for WooCommerce: from n/a through 1.4.2.	7.1	More Details
CVE-2024-51630	Cross-Site Request Forgery (CSRF) vulnerability in Lars Schenk Responsive Flickr Gallery allows Stored XSS.This issue affects Responsive Flickr Gallery: from n/a through 1.3.1.	7.1	More Details
CVE-2024-51693	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in laboratorio d'Avanguardia Search order by product SKU for WooCommerce allows Reflected XSS.This issue affects Search order by product SKU for WooCommerce: from n/a through 0.2.	7.1	More Details
CVE-2024-10676	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wojciech Borowicz Conversion Helper allows Reflected XSS.This issue affects Conversion Helper: from n/a through 1.12.	7.1	More Details
CVE-2024-51692	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Askew Brook Bing Search API Integration allows Reflected XSS.This issue affects Bing Search API Integration: from n/a through 0.3.3.	7.1	More Details
CVE-2024-51691	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Aryan Duntley Admin Amplify allows Reflected XSS.This issue affects Admin Amplify: from n/a through 1.3.0.	7.1	More Details
CVE-2024-51762	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Nightshift Creative PropertyShift allows Reflected XSS.This issue affects PropertyShift: from n/a through 1.0.0.	7.1	More Details
CVE-2024-51763	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Biplob Adhikari Team Showcase and Slider – Team Members Builder allows Reflected XSS.This issue affects Team Showcase and Slider – Team Members Builder: from n/a through 1.3.	7.1	More Details
CVE-2024-10203	Zohocorp ManageEngine EndPoint Central versions 11.3.2416.21 and below, 11.3.2428.9 and below are vulnerable to Arbitrary File Deletion in the agent installed machines.	7.0	More Details
CVE-2024-50592	An attacker with local access the to medical office computer can escalate his Windows user privileges to "NT AUTHORITY\SYSTEM" by exploiting a race condition in the Elefant Update Service during the repair or update process. When using the repair function, the service queries the server for a list of files and their hashes. In addition, instructions to execute binaries to finalize the repair process are included. The executables are executed as "NT AUTHORITY\SYSTEM" after they are copied over to the user writable installation folder (C:\Elefant1). This means that a user can overwrite either "PostESUUpdate.exe" or "Update_OpenJava.exe" in the time frame after the copy and before the execution of the final repair step. The overwritten executable is then executed as "NT AUTHORITY\SYSTEM".	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50234	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlegacy: Clear stale interrupts before resuming device iwl4965 fails upon resume from hibernation on my laptop. The reason seems to be a stale interrupt which isn't being cleared out before interrupts are enabled. We end up with a race beween the resume trying to bring things back up, and the restart work (queued form the interrupt handler) trying to bring things down. Eventually the whole thing blows up. Fix the problem by clearing out any stale interrupts before interrupts get enabled during resume. Here's a debug log of the indicent: [12.042589] ieee80211 phy0: il_isr ISR inta 0x00000080, enabled 0xaa00008b, fh 0x00000000 [12.042625] ieee80211 phy0: il4965_irq_tasklet inta 0x00000080, enabled 0x00000000, fh 0x00000000 [12.042651] iwl4965 0000:10:00.0: RF_KILL bit toggled to enable radio. [12.042653] iwl4965 0000:10:00.0: On demand firmware reload [12.042690] ieee80211 phy0: il4965_irq_tasklet End inta 0x00000000, enabled 0xaa00008b, fh 0x00000000, flags 0x00000282 [12.052207] ieee80211 phy0: il4965_mac_start enter [12.052212] ieee80211 phy0: il_prep_station Add STA to driver ID 31: ff:ff:ff:ff:ff:ff [12.052244] ieee80211 phy0: il4965_set_hw_ready hardware ready [12.052324] ieee80211 phy0: il_apm_init Init card's basic functions [12.052348] ieee80211 phy0: il_apm_init L1 Enabled; Disabling L0S [12.055727] ieee80211 phy0: il4965_load_bsm Begin load bsm [12.056140] ieee80211 phy0: il4965_verify_bsm Begin verify bsm [12.058642] ieee80211 phy0: il4965_verify_bsm BSM bootstrap uCode image OK [12.058721] ieee80211 phy0: il4965_load_bsm BSM write complete, poll 1 iterations [12.058734] ieee80211 phy0: __il4965_up iwl4965 is coming up [12.058737] ieee80211 phy0: il4965_mac_start Start UP work done. [12.058757] ieee80211 phy0: __il4965_down iwl4965 is going down [12.058761] ieee80211 phy0: il_scan_cancel_timeout Scan cancel timeout [12.058762] ieee80211 phy0: il_do_scan_abort Not performing scan to abort [12.058765] ieee80211 phy0: il_clear_ucode_stations Clearing ucode stations in driver [12.058767] ieee80211 phy0: il_clear_ucode_stations No active stations found to be cleared [12.058819] ieee80211 phy0: _il_apm_stop Stop card, put in low power state [12.058827] ieee80211 phy0: _il_apm_stop_master stop master [12.058864] ieee80211 phy0: il4965_clear_free_frames 0 frames on pre-allocated heap on clear. [12.058869] ieee80211 phy0: Hardware restart was requested [16.132299] iwl4965 0000:10:00.0: START_ALIVE timeout after 4000ms. [16.132303] ------------[cut here]------------ [16.132304] Hardware became unavailable upon resume. This could be a software issue prior to suspend or a hardware issue. [16.132338] WARNING: CPU: 0 PID: 181 at net/mac80211/util.c:1826 ieee80211_reconfig+0x8f/0x14b0 [mac80211] [16.132390] Modules linked in: ctr ccm sch_fq_codel xt_tcpudp xt_multiport xt_state iptable_filter iptable_nat nf_nat nf_conntrack nf_defrag_ipv4 ip_tables x_tables binfmt_misc joydev mousedev btusb btrtl btintel btbcm bluetooth ecdh_generic ecc iTCO_wdt i2c_dev iwl4965 iwlegacy coretemp snd_hda_codec_analog pcspkr psmouse mac80211 snd_hda_codec_generic libarc4 sdhci_pci cqhci sha256_generic sdhci libsha256 firewire_ohci snd_hda_intel snd_intel_dspcfg mmc_core snd_hda_codec snd_hwdep firewire_core led_class iosf_mbi snd_hda_core uhci_hcd lpc_ich crc_itu_t cfg80211 ehci_pci ehci_hcd snd_pcm usbcore mfd_core rfkill snd_timer snd usb_common soundcore video parport_pc parport intel_agp wmi intel_gtt backlight e1000e agpgart evdev [16.132456] CPU: 0 UID: 0 PID: 181 Comm: kworker/u8:6 Not tainted 6.11.0-cl+ #143 [16.132460] Hardware name: Hewlett-Packard HP Compaq 6910p/30BE, BIOS 68MCU Ver. F.19 07/06/2010 [16.132463] Workqueue: async async_run_entry_fn [16.132469] RIP: 0010:ieee80211_reconfig+0x8f/0x14b0 [mac80211] [16.132501] Code: da 02 00 0 ---truncated---	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50154	In the Linux kernel, the following vulnerability has been resolved: tcp/dccp: Don't use timer_pending() in reqsk_queue_unlink(). Martin KaFai Lau reported use-after-free [0] in reqsk_timer_handler(). """ We are seeing a use-after-free from a bpf prog attached to trace_tcp_retransmit_synack. The program passes the req->sk to the bpf_sk_storage_get_tracing kernel helper which does check for null before using it. """ The commit 83fccfc3940c ("inet: fix potential deadlock in reqsk_queue_unlink()") added timer_pending() in reqsk_queue_unlink() not to call del_timer_sync() from reqsk_timer_handler(), but it introduced a small race window. Before the timer is called, expire_timers() calls detach_timer(timer, true) to clear timer->entry.pprev and marks it as not pending. If reqsk_queue_unlink() checks timer_pending() just after expire_timers() calls detach_timer(), TCP will miss del_timer_sync(); the reqsk timer will continue running and send multiple SYN+ACKs until it expires. The reported UAF could happen if req->sk is close()d earlier than the timer expiration, which is 63s by default. The scenario would be 1. inet_csk_complete_hashdance() calls inet_csk_reqsk_queue_drop(), but del_timer_sync() is missed 2. reqsk timer is executed and scheduled again 3. req->sk is accept()ed and reqsk_put() decrements rsk_refcnt, but reqsk timer still has another one, and inet_csk_accept() does not clear req->sk for non-TFO sockets 4. sk is close()d 5. reqsk timer is executed again, and BPF touches req->sk Let's not use timer_pending() by passing the caller context to __inet_csk_reqsk_queue_drop(). Note that reqsk timer is pinned, so the issue does not happen in most use cases. [1] [0] BUG: KFENCE: use-after-free read in bpf_sk_storage_get_tracing+0x2e/0x1b0 Use-after-free read at 0x00000000a891fb3a (in kfence-#1): bpf_sk_storage_get_tracing+0x2e/0x1b0 bpf_prog_5ea3e95db6da0438_tcp_retransmit_synack+0x1d20/0x1dda bpf_trace_run2+0x4c/0xc0 tcp_rtx_synack+0xf9/0x100 reqsk_timer_handler+0xda/0x3d0 run_timer_softirq+0x292/0x8a0 irq_exit_rcu+0xf5/0x320 sysvec_apic_timer_interrupt+0x6d/0x80 asm_sysvec_apic_timer_interrupt+0x16/0x20 intel_idle_irq+0x5a/0xa0 cpuidle_enter_state+0x94/0x273 cpu_startup_entry+0x15e/0x260 start_secondary+0x8a/0x90 secondary_startup_64_no_verify+0xfa/0xfb kfence-#1: 0x00000000a72cc7b6-0x00000000d97616d9, size=2376, cache=TCPv6 allocated by task 0 on cpu 9 at 260507.901592s: sk_prot_alloc+0x35/0x140 sk_clone_lock+0x1f/0x3f0 inet_csk_clone_lock+0x15/0x160 tcp_create_openreq_child+0x1f/0x410 tcp_v6_syn_recv_sock+0x1da/0x700 tcp_check_req+0x1fb/0x510 tcp_v6_rcv+0x98b/0x1420 ipv6_list_rcv+0x2258/0x26e0 napi_complete_done+0x5b1/0x2990 mlx5e_napi_poll+0x2ae/0x8d0 net_rx_action+0x13e/0x590 irq_exit_rcu+0xf5/0x320 common_interrupt+0x80/0x90 asm_common_interrupt+0x22/0x40 cpuidle_enter_state+0xfb/0x273 cpu_startup_entry+0x15e/0x260 start_secondary+0x8a/0x90 secondary_startup_64_no_verify+0xfa/0xfb freed by task 0 on cpu 9 at 260507.927527s: rcu_core_si+0x4ff/0xf10 irq_exit_rcu+0xf5/0x320 sysvec_apic_timer_interrupt+0x6d/0x80 asm_sysvec_apic_timer_interrupt+0x16/0x20 cpuidle_enter_state+0xfb/0x273 cpu_startup_entry+0x15e/0x260 start_secondary+0x8a/0x90 secondary_startup_64_no_verify+0xfa/0xfb	7.0	More Details
CVE-2024-43643	Windows USB Video Class System Driver Elevation of Privilege Vulnerability	6.8	More Details
CVE-2024-36140	A vulnerability has been identified in OZW672 (All versions < V5.2), OZW772 (All versions < V5.2). The user accounts tab of affected devices is vulnerable to stored cross-site scripting (XSS) attacks. This could allow an authenticated remote attacker to inject arbitrary JavaScript code that is later executed by another authenticated victim user with potential higher privileges than the attacker.	6.8	More Details
CVE-2024-40240	An incorrect access control issue in HomeServe Home Repair' android app - 3.3.4 allows a physically proximate attacker to escalate privileges via the fingerprint authentication function.	6.8	More Details
CVE-2024-45759	Dell PowerProtect Data Domain, versions prior to 8.1.0.0, 7.13.1.10, 7.10.1.40, and 7.7.5.50, contains an escalation of privilege vulnerability. A local low privileged attacker could potentially exploit this vulnerability, leading to unauthorized execution of certain commands to overwrite system config of the application. Exploitation may lead to denial of service of system.	6.8	More Details
CVE-2024-43637	Windows USB Video Class System Driver Elevation of Privilege Vulnerability	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43638	Windows USB Video Class System Driver Elevation of Privilege Vulnerability	6.8	More Details
CVE-2024-43634	Windows USB Video Class System Driver Elevation of Privilege Vulnerability	6.8	More Details
CVE-2024-40239	An incorrect access control issue in Life: Personal Diary, Journal android app 17.5.0 allows a physically proximate attacker to escalate privileges via the fingerprint authentication function.	6.8	More Details
CVE-2024-43449	Windows USB Video Class System Driver Elevation of Privilege Vulnerability	6.8	More Details
CVE-2024-8881	A post-authentication command injection vulnerability in the CGI program in the Zyxel GS1900-48 switch firmware version V2.80(AAHN.1)C0 and earlier could allow an authenticated, LAN-based attacker with administrator privileges to execute some operating system (OS) commands on an affected device by sending a crafted HTTP request.	6.8	More Details
CVE-2024-49406	Improper validation of integrity check value in Blockchain Keystore prior to version 1.3.16 allows local attackers to modify transaction. Root privilege is required for triggering this vulnerability.	6.7	More Details
CVE-2024-32118	Multiple improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerabilities [CWE-78] in Fortinet FortiManager version 7.4.0 through 7.4.2 and before 7.2.5, Fortinet FortiAnalyzer version 7.4.0 through 7.4.2 and before 7.2.5 and Fortinet FortiAnalyzer-BigData before 7.4.0 allows an authenticated privileged attacker to execute unauthorized code or commands via crafted CLI requests.	6.7	More Details
CVE-2024-31496	A stack-based buffer overflow vulnerability [CWE-121] in Fortinet FortiManager version 7.4.0 through 7.4.2 and before 7.2.5, FortiAnalyzer version 7.4.0 through 7.4.2 and before 7.2.5 and FortiAnalyzer-BigData 7.4.0 and before 7.2.7 allows a privileged attacker to execute unauthorized code or commands via crafted CLI requests.	6.7	More Details
CVE-2024-43631	Windows Secure Kernel Mode Elevation of Privilege Vulnerability	6.7	More Details
CVE-2024-43646	Windows Secure Kernel Mode Elevation of Privilege Vulnerability	6.7	More Details
CVE-2024-43645	Windows Defender Application Control (WDAC) Security Feature Bypass Vulnerability	6.7	More Details
CVE-2024-49044	Visual Studio Elevation of Privilege Vulnerability	6.7	More Details
CVE-2024-28728	Cross Site Scripting vulnerability in DLink DWR 2000M 5G CPE With Wifi 6 Ax1800 and Dlink DWR 5G CPE DWR-2000M_1.34ME allows a local attacker to obtain sensitive information via a crafted payload to the WiFi SSID Name field.	6.6	More Details
CVE-2024-34681	Improper input validation in BluetoothAdapter prior to SMR Nov-2024 Release 1 allows local attackers to cause local permanent denial of service on Galaxy Watch.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51662	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Modernaweb Studio Black Widgets For Elementor allows Stored XSS.This issue affects Black Widgets For Elementor: from n/a through 1.3.6.	6.5	More Details
CVE-2024-51585	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in NicheAddons Sales Page Addon – Elementor & Beaver Builder allows Stored XSS.This issue affects Sales Page Addon – Elementor & Beaver Builder: from n/a through 1.4.2.	6.5	More Details
CVE-2024-51586	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BRAFT Elementary Addons allows Stored XSS.This issue affects Elementary Addons: from n/a through 2.0.4.	6.5	More Details
CVE-2024-51587	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Softfirm Definitive Addons for Elementor allows Stored XSS.This issue affects Definitive Addons for Elementor: from n/a through 1.5.16.	6.5	More Details
CVE-2024-51629	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in MetricThemes Header Footer Composer for Elementor allows DOM-Based XSS.This issue affects Header Footer Composer for Elementor: from n/a through 1.0.4.	6.5	More Details
CVE-2024-51588	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themehat Super Addons for Elementor allows DOM-Based XSS.This issue affects Super Addons for Elementor: from n/a through 1.0.	6.5	More Details
CVE-2024-51589	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in wpcirqle Bigmart Elements allows DOM-Based XSS.This issue affects Bigmart Elements: from n/a through 1.0.3.	6.5	More Details
CVE-2024-51673	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in HasThemes HT Politic allows DOM-Based XSS.This issue affects HT Politic: from n/a through 2.4.4.	6.5	More Details
CVE-2024-51590	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Hoosoft Hoo Addons for Elementor allows DOM-Based XSS.This issue affects Hoo Addons for Elementor: from n/a through 1.0.6.	6.5	More Details
CVE-2024-51577	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Camunda Services GmbH bpmn.Io allows Stored XSS.This issue affects bpmn.Io: from n/a through 1.0.	6.5	More Details
CVE-2024-51576	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPZA AMP Img Shortcode allows Stored XSS.This issue affects AMP Img Shortcode: from n/a through 1.0.1.	6.5	More Details
CVE-2024-20457	A vulnerability in the logging component of Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an authenticated, remote attacker to view sensitive information in clear text on an affected system. This vulnerability is due to the storage of unencrypted credentials in certain logs. An attacker could exploit this vulnerability by accessing the logs on an affected system and obtaining credentials that they may not normally have access to. A successful exploit could allow the attacker to access sensitive information from the device.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9681	When curl is asked to use HSTS, the expiry time for a subdomain might overwrite a parent domain's cache entry, making it end sooner or later than otherwise intended. This affects curl using applications that enable HSTS and use URLs with the insecure `HTTP://` scheme and perform transfers with hosts like `x.example.com` as well as `example.com` where the first host is a subdomain of the second host. (The HSTS cache either needs to have been populated manually or there needs to have been previous HTTPS accesses done as the cache needs to have entries for the domains involved to trigger this problem.) When `x.example.com` responds with `Strict-Transport-Security:` headers, this bug can make the subdomain's expiry timeout *bleed over* and get set for the parent domain `example.com` in curl's HSTS cache. The result of a triggered bug is that HTTP accesses to `example.com` get converted to HTTPS for a different period of time than what was asked for by the origin server. If `example.com` for example stops supporting HTTPS at its expiry time, curl might then fail to access `http://example.com` until the (wrongly set) timeout expires. This bug can also expire the parent's entry *earlier*, thus making curl inadvertently switch back to insecure HTTP earlier than otherwise intended.	6.5	More Details
CVE-2024-11110	Inappropriate implementation in Extensions in Google Chrome prior to 131.0.6778.69 allowed a remote attacker to bypass site isolation via a crafted Chrome Extension. (Chromium security severity: High)	6.5	More Details
CVE-2024-51571	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in MasterBip MasterBip para Elementor allows DOM-Based XSS.This issue affects MasterBip para Elementor: from n/a through 1.6.3.	6.5	More Details
CVE-2024-51572	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Peter Shaw LH QR Codes allows Stored XSS.This issue affects LH QR Codes: from n/a through 1.06.	6.5	More Details
CVE-2024-51573	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Matthew Lillistone ML Responsive Audio player with playlist Shortcode allows Stored XSS.This issue affects ML Responsive Audio player with playlist Shortcode: from n/a through 0.2.	6.5	More Details
CVE-2024-51574	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Simple Goods allows Stored XSS.This issue affects Simple Goods: from n/a through 0.1.3.	6.5	More Details
CVE-2024-51575	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Abdullah Extender All In One For Elementor allows Stored XSS.This issue affects Extender All In One For Elementor: from n/a through 1.0.3.	6.5	More Details
CVE-2024-52356	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Webangon The Pack Elementor addons allows Stored XSS.This issue affects The Pack Elementor addons: from n/a through 2.1.0.	6.5	More Details
CVE-2024-52357	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in LIQUID DESIGN Ltd. LIQUID BLOCKS allows Stored XSS.This issue affects LIQUID BLOCKS: from n/a through 1.2.0.	6.5	More Details
CVE-2024-52358	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Cyberchimps Responsive Addons for Elementor allows DOM-Based XSS.This issue affects Responsive Addons for Elementor: from n/a through 1.5.4.	6.5	More Details
CVE-2024-52350	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CRM 2go allows DOM-Based XSS.This issue affects CRM 2go: from n/a through 1.0.	6.5	More Details
CVE-2024-52351	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Boston University (IS&T) BU Slideshow allows Stored XSS.This issue affects BU Slideshow: from n/a through 2.3.10.	6.5	More Details
CVE-2024-52352	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Andrew Milo Postcasa Shortcode allows DOM-Based XSS.This issue affects Postcasa Shortcode: from n/a through 1.0.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-52353	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Gabriel Serafini Christian Science Bible Lesson Subjects allows DOM-Based XSS.This issue affects Christian Science Bible Lesson Subjects: from n/a through 2.0.	6.5	More Details
CVE-2024-52354	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Cool Plugins Web Stories Widgets For Elementor allows Stored XSS.This issue affects Web Stories Widgets For Elementor: from n/a through 1.1.	6.5	More Details
CVE-2024-52355	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Hyumika OSM – OpenStreetMap allows Stored XSS.This issue affects OSM – OpenStreetMap: from n/a through 6.1.2.	6.5	More Details
CVE-2021-27704	Appspace 6.2.4 is affected by Incorrect Access Control via the Appspace Web Portal password reset page.	6.5	More Details
CVE-2024-51578	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Luca Paggetti 3D Presentation allows Stored XSS.This issue affects 3D Presentation: from n/a through 1.0.	6.5	More Details
CVE-2024-51584	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Anas Edreesi Marquee Elementor with Posts allows DOM-Based XSS.This issue affects Marquee Elementor with Posts: from n/a through 1.2.0.	6.5	More Details
CVE-2024-51591	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in wpgrids Slicko allows DOM-Based XSS.This issue affects Slicko: from n/a through 1.2.0.	6.5	More Details
CVE-2024-51583	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in KentoThemes Kento Ads Rotator allows Stored XSS.This issue affects Kento Ads Rotator: from n/a through 1.3.	6.5	More Details
CVE-2024-51592	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in bnayawpguy Meta Store Elements allows DOM-Based XSS.This issue affects Meta Store Elements: from n/a through 1.0.9.	6.5	More Details
CVE-2024-51593	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Glopium Studio Курс валют UAH allows Stored XSS.This issue affects Курс валют UAH: from n/a through 2.0.	6.5	More Details
CVE-2024-51594	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Rafel Sansó Gmap Point List allows Stored XSS.This issue affects Gmap Point List: from n/a through 1.1.2.	6.5	More Details
CVE-2024-51595	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in sksdev SKSDEV Toolkit allows Stored XSS.This issue affects SKSDEV Toolkit: from n/a through 1.0.0.	6.5	More Details
CVE-2024-51596	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Nilesh Shiragave Business allows Stored XSS.This issue affects Business: from n/a through 1.3.	6.5	More Details
CVE-2024-51597	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ThemeShark ThemeShark Templates & Widgets for Elementor allows Stored XSS.This issue affects ThemeShark Templates & Widgets for Elementor: from n/a through 1.1.7.	6.5	More Details
CVE-2024-51598	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kendysond Selar.Co Widget allows DOM-Based XSS.This issue affects Selar.Co Widget: from n/a through 1.2.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51599	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Russell Albin Simple Business Manager allows Stored XSS.This issue affects Simple Business Manager: from n/a through 4.6.7.4.	6.5	More Details
CVE-2024-51603	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Mircea N. NMR Strava activities allows DOM-Based XSS.This issue affects NMR Strava activities: from n/a through 1.0.6.	6.5	More Details
CVE-2024-51604	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Carlo Andro Mabugay Media Modal allows DOM-Based XSS.This issue affects Media Modal: from n/a through 1.0.2.	6.5	More Details
CVE-2024-51605	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Genoo, LLC Genoo allows DOM-Based XSS.This issue affects Genoo: from n/a through 6.0.10.	6.5	More Details
CVE-2024-51988	RabbitMQ is a feature rich, multi-protocol messaging and streaming broker. In affected versions queue deletion via the HTTP API was not verifying the `configure` permission of the user. Users who had all of the following: 1. Valid credentials, 2. Some permissions for the target virtual host & 3. HTTP API access. could delete queues it had no (deletion) permissions for. This issue has been addressed in version 3.12.11 of the open source rabbitMQ release and in versions 1.5.2, 3.13.0, and 4.0.0 of the tanzu release. Users are advised to upgrade. Users unable to upgrade may disable management plugin and use, for example, Prometheus and Grafana for monitoring.	6.5	More Details
CVE-2024-51609	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Elsner Technologies Pvt. Ltd. Emoji Shortcode allows Stored XSS.This issue affects Emoji Shortcode: from n/a through 1.0.0.	6.5	More Details
CVE-2024-51610	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in SEO Themes Display Terms Shortcode allows Stored XSS.This issue affects Display Terms Shortcode: from n/a through 1.0.4.	6.5	More Details
CVE-2024-51627	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kaedinger Audio Comparison Lite audio-comparison-lite allows Stored XSS.This issue affects Audio Comparison Lite: from n/a through 3.4.	6.5	More Details
CVE-2024-51751	Gradio is an open-source Python package designed to enable quick builds of a demo or web application. If File or UploadButton components are used as a part of Gradio application to preview file content, an attacker with access to the application might abuse these components to read arbitrary files from the application server. This issue has been addressed in release version 5.5.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2024-20537	A vulnerability in the web-based management interface of Cisco ISE could allow an authenticated, remote attacker to bypass the authorization mechanisms for specific administrative functions. This vulnerability is due to a lack of server-side validation of Administrator permissions. An attacker could exploit this vulnerability by submitting a crafted HTTP request to an affected system. A successful exploit could allow the attacker to conduct administrative functions beyond their intended access level. To exploit this vulnerability, an attacker would need Read-Only Administrator credentials.	6.5	More Details
CVE-2024-51580	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CleverSoft Clever Addons for Elementor allows Stored XSS.This issue affects Clever Addons for Elementor: from n/a through 2.2.1.	6.5	More Details
CVE-2024-51581	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in NicheAddons Restaurant & Cafe Addon for Elementor allows Stored XSS.This issue affects Restaurant & Cafe Addon for Elementor: from n/a through 1.5.6.	6.5	More Details
CVE-2024-51628	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in EzyOnlineBookings EzyOnlineBookings Online Booking System Widget allows DOM-Based XSS.This issue affects EzyOnlineBookings Online Booking System Widget: from n/a through 1.3.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51055	An issue Hoosk v1.7.1 allows a remote attacker to execute arbitrary code via a crafted script to the config.php component.	6.5	More Details
CVE-2024-44765	An Improper Authorization (Access Control Misconfiguration) vulnerability in MGT-COMMERCE GmbH CloudPanel v2.0.0 to v2.4.2 allows low-privilege users to bypass access controls and gain unauthorized access to sensitive configuration files and administrative functionality.	6.5	More Details
CVE-2024-42372	Due to missing authorization check in SAP NetWeaver AS Java (System Landscape Directory) an unauthorized user can read and modify some restricted global SLD configurations causing low impact on confidentiality and integrity of the application.	6.5	More Details
CVE-2024-43633	Windows Hyper-V Denial of Service Vulnerability	6.5	More Details
CVE-2024-9262	The User Meta – User Profile Builder and User management plugin plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.1 via the getUser() due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Contributor-level access and above, to obtain user meta values from form fields. Please note that this requires a site administrator to create a form that displays potentially sensitive information like password hashes. This may also be exploited by unauthenticated users if the 'user-meta-public-profile' shortcode is used insecurely.	6.5	More Details
CVE-2024-51622	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Experts Team WP EASY RECIPE allows Stored XSS.This issue affects WP EASY RECIPE: from n/a through 1.6.	6.5	More Details
CVE-2024-51566	The NVMe driver queue processing is vulernable to guest-induced infinite loops.	6.5	More Details
CVE-2024-51565	The hda driver is vulnerable to a buffer over-read from a guest-controlled value.	6.5	More Details
CVE-2024-51563	The virtio_vq_recordon function is subject to a time-of-check to time-of-use (TOCTOU) race condition.	6.5	More Details
CVE-2024-51787	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in QuomodoSoft ElementsReady Addons for Elementor allows Stored XSS.This issue affects ElementsReady Addons for Elementor: from n/a through 6.4.3.	6.5	More Details
CVE-2024-51030	A SQL injection vulnerability in manage_client.php and view_cab.php of Sourcecodester Cab Management System 1.0 allows remote attackers to execute arbitrary SQL commands via the id parameter, leading to unauthorized access and potential compromise of sensitive data within the database.	6.5	More Details
CVE-2024-51786	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BestWebSoft Realty by BestWebSoft allows Stored XSS.This issue affects Realty by BestWebSoft: from n/a through 1.1.5.	6.5	More Details
CVE-2024-51409	Buffer Overflow vulnerability in Tenda O3 v.1.0.0.5 allows a remote attacker to cause a denial of service via a network packet in a fixed format to a router running the corresponding version of the firmware.	6.5	More Details
CVE-2024-10294	The CE21 Suite plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ce21_single_sign_on_save_api_settings' function in versions up to, and including, 2.2.0. This makes it possible for unauthenticated attackers to change plugin settings.	6.5	More Details
CVE-2024-46947	Northern.tech Mender before 3.6.6 and 3.7.x before 3.7.7 allows SSRF.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9999	In WS_FTP Server versions before 8.8.9 (2022.0.9), an Incorrect Implementation of Authentication Algorithm in the Web Transfer Module allows users to skip the second-factor verification and log in with username and password only.	6.5	More Details
CVE-2024-51562	The NVMe driver function nvme_opc_get_log_page is vulnerable to a buffer over-read from a guest-controlled value.	6.5	More Details
CVE-2024-51675	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in aThemes aThemes Addons for Elementor allows DOM-Based XSS.This issue affects aThemes Addons for Elementor: from n/a through 1.0.7.	6.5	More Details
CVE-2024-51618	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in DuoGeek Custom Admin Menu allows Stored XSS.This issue affects Custom Admin Menu: from n/a through 1.0.0.	6.5	More Details
CVE-2024-51616	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Nazmul Hasan Rupok AwesomePress allows Stored XSS.This issue affects AwesomePress: from n/a through 1.0.	6.5	More Details
CVE-2024-51614	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Aajoda Aajoda Testimonials allows Stored XSS.This issue affects Aajoda Testimonials: from n/a through 2.2.2.	6.5	More Details
CVE-2024-51613	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Andrew Connell TradeMe widgets allows Stored XSS.This issue affects TradeMe widgets: from n/a through 1.2.	6.5	More Details
CVE-2024-51612	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Ken Charity Reftagger Shortcode allows Stored XSS.This issue affects Reftagger Shortcode: from n/a through 1.1.	6.5	More Details
CVE-2024-48010	Dell PowerProtect DD, versions prior to 8.1.0.0, 7.13.1.10, 7.10.1.40, and 7.7.5.50, contains an access control vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to escalation of privilege on the application.	6.5	More Details
CVE-2024-51611	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Miguel Peixe WP Feature Box allows Stored XSS.This issue affects WP Feature Box: from n/a through 0.1.3.	6.5	More Details
CVE-2024-43451	NTLM Hash Disclosure Spoofing Vulnerability	6.5	More Details
CVE-2024-51674	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in TemplatesCoder Sastra Essential Addons for Elementor allows DOM-Based XSS.This issue affects Sastra Essential Addons for Elementor: from n/a through 1.0.5.	6.5	More Details
CVE-2024-52296	libosdp is an implementation of IEC 60839-11-5 OSDP (Open Supervised Device Protocol) and provides a C library with support for C++, Rust and Python3. At ospd_common.c, on the osdp_reply_name function, any reply id between REPLY_ACK and REPLY_XRD is valid, but names array do not declare all of the range. On a case of an undefined reply id within the range, name will be null (name = names[reply_id - REPLY_ACK];). Null name will casue a crash on next line: if (name[0] == '\0') as null[0] is invalid. As this logic is not limited to a secure connection, attacker may trigger this vulnerability without any prior knowledge. This issue is fixed in 2.4.0.	6.5	More Details
CVE-2024-10186	The Event post plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's events_cal shortcode in all versions up to, and including, 5.9.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10814	The Code Embed plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 2.5 via the ce_get_file() function. This makes it possible for authenticated attackers, with contributor-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.	6.4	More Details
CVE-2024-10269	The Easy SVG Support plugin for WordPress is vulnerable to Stored Cross-Site Scripting via REST API SVG File uploads in all versions up to, and including, 3.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-10621	The Simple Shortcode for Google Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's pw_map shortcode in all versions up to, and including, 1.5.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-8323	The Pricing Tables WordPress Plugin – Easy Pricing Tables plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘fontFamily’ attribute in all versions up to, and including, 3.2.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with 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-2024-10168	The Active Products Tables for WooCommerce. Use constructor to create tables plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's woot_button shortcode in all versions up to, and including, 1.0.6.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-10187	The myCred – Loyalty Points and Rewards plugin for WordPress and WooCommerce – Give Points, Ranks, Badges, Cashback, WooCommerce rewards, and WooCommerce credits for Gamification plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's mycred_link shortcode in all versions up to, and including, 2.7.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-51722	A local privilege escalation vulnerability in the SecuSUITE Server (System Configuration) of SecuSUITE versions 5.0.420 and earlier could allow a successful attacker that had gained control of code running under one of the system accounts listed in the configuration file to potentially issue privileged script commands.	6.4	More Details
CVE-2024-10715	The MapPress Maps for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Map block in all versions up to, and including, 2.94.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-10325	The Elementor Header & Footer Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via REST API SVG File uploads in all versions up to, and including, 1.6.45 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-48952	An issue was discovered in Logpoint before 7.5.0. SOAR uses a static JWT secret key to generate tokens that allow access to SOAR API endpoints without authentication. This static key vulnerability enables attackers to create custom JWT secret keys for unauthorized access to these endpoints.	6.4	More Details
CVE-2024-48954	An issue was discovered in Logpoint before 7.5.0. Unvalidated input during the EventHub Collector setup by an authenticated user leads to Remote Code execution.	6.4	More Details
CVE-2024-49408	Out-of-bounds write in usb driver prior to Firmware update Sep-2024 Release on Galaxy S24 allows local attackers to write out-of-bounds memory. System privilege is required for triggering this vulnerability.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10538	The Happy Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the before_label parameter in the Image Comparison widget in all versions up to, and including, 3.12.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-9270	The Lenxel Core for Lenxel(LNX) LMS plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-45088	IBM Maximo Asset Management 7.6.1.3 is vulnerable to stored cross-site scripting. This vulnerability allows authenticated users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	6.4	More Details
CVE-2024-49409	Out-of-bounds write in Battery Full Capacity node prior to Firmware update Sep-2024 Release on Galaxy S24 allows local attackers to write out-of-bounds memory. System privilege is required for triggering this vulnerability.	6.4	More Details
CVE-2024-8960	The Cowidgets – Elementor Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.2.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-10179	The Slickstream: Engagement and Conversions plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's slick-grid shortcode in all versions up to, and including, 1.4.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-10323	The JetWidgets For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via REST API SVG File uploads in all versions up to, and including, 1.0.18 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-8442	The Prime Slider – Addons For Elementor (Revolution of a slider, Hero Slider, Ecommerce Slider) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Blog widget in all versions up to, and including, 3.15.18 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-2024-11096	A vulnerability, which was classified as critical, was found in code-projects Task Manager 1.0. This affects an unknown part of the file /newProject.php. The manipulation of the argument projectName 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-2024-47595	An attacker who gains local membership to sapsys group could replace local files usually protected by privileged access. On successful exploitation the attacker could cause high impact on confidentiality and integrity of the application.	6.3	More Details
CVE-2024-9902	A flaw was found in Ansible. The ansible-core `user` module can allow an unprivileged user to silently create or replace the contents of any file on any system path and take ownership of it when a privileged user executes the `user` module against the unprivileged user's home directory. If the unprivileged user has traversal permissions on the directory containing the exploited target file, they retain full control over the contents of the file as its owner.	6.3	More Details
CVE-2024-11051	A vulnerability was found in AMTT Hotel Broadband Operation System up to 3.0.3.151204. It has been classified as critical. Affected is an unknown function of the file /manager/frontdesk/online_status.php. The manipulation of the argument AccountID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-11059	A vulnerability was found in Project Worlds Free Download Online Shopping System up to 192.168.1.88. It has been rated as critical. This issue affects some unknown processing of the file /online-shopping-webvsite-in-php-master/success.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-2024-10990	A vulnerability classified as critical was found in SourceCodester Online Veterinary Appointment System 1.0. This vulnerability affects unknown code of the file /admin/services/view_service.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-2020-11916	An issue was discovered in Siime Eye 14.1.00000001.3.330.0.0.3.14. The password for the root user is hashed using an old and deprecated hashing technique. Because of this deprecated hashing, the success probability of an attacker in an offline cracking attack is greatly increased.	6.3	More Details
CVE-2024-52311	Authentication tokens issued via Cognito in data.all are not invalidated on log out, allowing for previously authenticated user to continue execution of authorized API Requests until token is expired.	6.3	More Details
CVE-2024-10987	A vulnerability was found in code-projects E-Health Care System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /Doctor/user_appointment.php. The manipulation of the argument schedule_id/schedule_date/schedule_day/start_time/end_time/booking 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-2024-11076	A vulnerability, which was classified as critical, has been found in code-projects Job Recruitment 1.0. This issue affects some unknown processing of the file /activation.php. The manipulation of the argument e_hash 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-2024-10966	A vulnerability, which was classified as critical, has been found in TOTOLINK X18 9.1.0cu.2024_B20220329. Affected by this issue is some unknown functionality of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument enable leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-11060	A vulnerability classified as critical has been found in Jinher Network Collaborative Management Platform 金和数字化智能办公平台 1.0. Affected is an unknown function of the file /C6/JHSoft.Web.AcceptAip/AcceptShow.aspx/. 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-2024-10989	A vulnerability classified as critical has been found in code-projects E-Health Care System 1.0. This affects an unknown part of the file /Admin/detail.php. The manipulation of the argument s_id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory confuses the vulnerability class of this issue.	6.3	More Details
CVE-2024-11074	A vulnerability classified as critical was found in itsourcecode Tailoring Management System 1.0. This vulnerability affects unknown code of the file /incadd.php. The manipulation of the argument inccat/desc/date/amount leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only mentions the parameter "inccat" to be affected. But it must be assumed "desc", "date", and "amount" are affected as well.	6.3	More Details
CVE-2024-10919	A vulnerability has been found in didi Super-Jacoco 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /cov/triggerUnitCover. The manipulation of the argument uuid leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-11121	A vulnerability classified as critical was found in 上海灵当信息科技有限公司 Lingdang CRM up to 8.6.4.3. Affected by this vulnerability is an unknown functionality of the file /crm/WeiXinApp/marketing/index.php?module=Users&action=getActionList. The manipulation of the argument userid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-11122	A vulnerability, which was classified as critical, has been found in 上海灵当信息科技有限公司 Lingdang CRM up to 8.6.4.3. Affected by this issue is some unknown functionality of the file /crm/wechatSession/index.php?msgid=1&operation=upload. The manipulation of the argument file leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-46894	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 3). The affected application does not properly validate authorization of a user to query the "/api/sftp/users" endpoint. This could allow an authenticated remote attacker to gain knowledge about the list of configured users of the SFTP service and also modify that configuration.	6.3	More Details
CVE-2024-10993	A vulnerability, which was classified as critical, was found in Codezips Online Institute Management System 1.0. Affected is an unknown function of the file /manage_website.php. The manipulation of the argument website_image leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-11046	A vulnerability was found in D-Link DI-8003 16.07.16A1. It has been classified as critical. Affected is the function upgrade_filter_asp of the file /upgrade_filter.asp. The manipulation of the argument path leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10997	A vulnerability was found in 1000 Projects Bookstore Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /book_list.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-2024-10994	A vulnerability has been found in Codezips Online Institute Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /edit_user.php. The manipulation of the argument image leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-11054	A vulnerability classified as critical was found in SourceCodester Simple Music Cloud Community System 1.0. This vulnerability affects unknown code of the file /music/ajax.php?action=signup. The manipulation of the argument pp leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-11127	A vulnerability was found in code-projects Job Recruitment up to 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file admin.php. The manipulation of the argument userid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10964	A vulnerability classified as critical has been found in emqx neuron up to 2.10.0. Affected is the function handle_add_plugin in the library cmd.library of the file plugins/restful/plugin_handle.c. The manipulation leads to buffer overflow. It is possible to launch the attack remotely. It is recommended to apply a patch to fix this issue.	6.3	More Details
CVE-2024-36064	The NLL com.nll.cb (aka ACR Phone) application through 0.330-playStore-NoAccessibility-arm8 for Android allows any installed application (with no permissions) to place phone calls without user interaction by sending a crafted intent via the com.nll.cb.dialer.dialer.DialerActivity component.	6.2	More Details
CVE-2019-20472	An issue was discovered on One2Track 2019-12-08 devices. Any SIM card used with the device cannot have a PIN configured. If a PIN is configured, the device simply produces a "Remove PIN and restart!" message, and cannot be used. This makes it easier for an attacker to use the SIM card by stealing the device.	6.2	More Details
CVE-2024-35420	wac commit 385e1 was discovered to contain a heap overflow.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38203	Windows Package Library Manager Information Disclosure Vulnerability	6.2	More Details
CVE-2024-35418	wac commit 385e1 was discovered to contain a heap overflow via the setup_call function at /wac-asan/wa.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted wasm file.	6.2	More Details
CVE-2024-35410	wac commit 385e1 was discovered to contain a heap overflow via the interpret function at /wac-asan/wa.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted wasm file.	6.2	More Details
CVE-2024-50251	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_payload: sanitize offset and length before calling skb_checksum() If access to offset + length is larger than the skbuff length, then skb_checksum() triggers BUG_ON(). skb_checksum() internally subtracts the length parameter while iterating over skbuff, BUG_ON(len) at the end of it checks that the expected length to be included in the checksum calculation is fully consumed.	6.2	More Details
CVE-2024-10683	The Contact Form 7 – PayPal & Stripe Add-on plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg & remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.3.1. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. This is only exploitable when the leave a review notice is present in the dashboard.	6.1	More Details
CVE-2024-10647	The WS Form LITE – Drag & Drop Contact Form Builder for WordPress plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.9.244. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-50990	A Reflected Cross Site Scriptng (XSS) vulnerability was found in /omrs/user/search.php in PHPGurukul Online Marriage Registration System v1.0, which allows remote attackers to execute arbitrary code via the "searchdata" POST request parameter.	6.1	More Details
CVE-2024-50601	Persistent and reflected XSS vulnerabilities in the themeMode cookie and _h URL parameter of Axigen Mail Server up to version 10.5.28 allow attackers to execute arbitrary Javascript. Exploitation could lead to session hijacking, data leakage, and further exploitation via a multi-stage attack. Fixed in versions 10.3.3.67, 10.4.42, and 10.5.29.	6.1	More Details
CVE-2024-51213	Cross Site Scripting vulnerability in Online Shop Store v.1.0 allows a remote attacker to execute arbitrary code via the login.php component.	6.1	More Details
CVE-2024-10837	The SysBasics Customize My Account for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘tab’ parameter in all versions up to, and including, 2.7.29 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-51434	Inconsistent <plaintext> tag parsing allows for XSS in Froala WYSIWYG editor 4.3.0 and earlier.	6.1	More Details
CVE-2024-10685	The Contact Form 7 Redirect & Thank You Page plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in all versions up to, and including, 1.0.6 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1932	A flaw was found in hibernate-validator's 'isValid' method in the org.hibernate.validator.internal.constraintvalidators.hv.SafeHtmlValidator class, which can be bypassed by omitting the tag ending in a less-than character. Browsers may render an invalid html, allowing HTML injection or Cross-Site-Scripting (XSS) attacks.	6.1	More Details
CVE-2024-9357	The xili-tidy-tags plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'action' parameter in all versions up to, and including, 1.12.04 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-20538	A vulnerability in the web-based management interface of Cisco ISE could allow an unauthenticated, remote attacker to conduct an XSS attack against a user of the interface. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface on an affected system to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details
CVE-2024-9841	A Reflected Cross-Site Scripting (XSS) vulnerability has been identified in OpenText ArcSight Management Center and ArcSight Platform. The vulnerability could be remotely exploited.	6.1	More Details
CVE-2024-50599	A reflected Cross-Site Scripting (XSS) vulnerability has been identified in Zimbra Collaboration Suite (ZCS) 8.8.15, affecting one of the webmail calendar endpoints. This arises from improper handling of user-supplied input, allowing an attacker to inject malicious code that is reflected back in the HTML response.	6.1	More Details
CVE-2024-11004	Reflected XSS in Ivanti Connect Secure before version 22.7R2.1 and Ivanti Policy Secure before version 22.7R1.1 allows a remote unauthenticated attacker to obtain admin privileges. User interaction is required.	6.1	More Details
CVE-2024-11019	Webopac from Grand Vice info has a Reflected Cross-site Scripting vulnerability, allowing unauthenticated remote attackers to execute arbitrary JavaScript code in the user's browser through phishing techniques.	6.1	More Details
CVE-2024-10265	The Form Maker by 10Web – Mobile-Friendly Drag & Drop Contact Form Builder plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.15.30. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-9226	The Landing Page Cat – Coming Soon Page, Maintenance Page & Squeeze Pages plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.7.6. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-20525	A vulnerability in the web-based management interface of Cisco ISE could allow an unauthenticated, remote attacker to conduct an XSS attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details
CVE-2024-20511	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9934	The Wp-ImageZoom WordPress plugin through 1.1.0 does not sanitise and escape some parameters before outputting them back in a page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2024-10876	The Charitable – Donation Plugin for WordPress – Fundraising with Recurring Donations & More plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg & remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.8.3. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-20530	A vulnerability in the web-based management interface of Cisco ISE could allow an unauthenticated, remote attacker to conduct an XSS attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details
CVE-2024-2207	Potential vulnerabilities have been identified in the audio package for certain HP PC products using the Sound Research SECOMN64 driver, which might allow escalation of privilege. Sound Research has released driver updates to mitigate the potential vulnerabilities.	6.0	More Details
CVE-2024-9836	The RSS Feed Widget WordPress plugin before 3.0.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.9	More Details
CVE-2024-38264	Microsoft Virtual Hard Disk (VHDX) Denial of Service Vulnerability	5.9	More Details
CVE-2024-51663	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Bricksable Bricksable for Bricks Builder allows Stored XSS.This issue affects Bricksable for Bricks Builder: from n/a through 1.6.59.	5.9	More Details
CVE-2024-34678	Out-of-bounds write in libsapeextractor.so prior to SMR Nov-2024 Release 1 allows local attackers to cause memory corruption.	5.9	More Details
CVE-2024-51670	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in JS Help Desk JS Help Desk – Best Help Desk & Support Plugin allows Stored XSS.This issue affects JS Help Desk – Best Help Desk & Support Plugin: from n/a through 2.8.7.	5.9	More Details
CVE-2024-51664	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Mark Kinchin Beds24 Online Booking allows Stored XSS.This issue affects Beds24 Online Booking: from n/a through 2.0.25.	5.9	More Details
CVE-2024-51668	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Mark Tilly MyCurator Content Curation allows Stored XSS.This issue affects MyCurator Content Curation: from n/a through 3.78.	5.9	More Details
CVE-2024-33505	A heap-based buffer overflow in Fortinet FortiAnalyzer version 7.4.0 through 7.4.2, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, FortiManager version 7.4.0 through 7.4.2, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14 allows attacker to escalation of privilege via specially crafted http requests	5.6	More Details
CVE-2024-50206	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: mtk_eth_soc: fix memory corruption during fq dma init The loop responsible for allocating up to MTK_FQ_DMA_LENGTH buffers must only touch as many descriptors, otherwise it ends up corrupting unrelated memory. Fix the loop iteration count accordingly.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50224	In the Linux kernel, the following vulnerability has been resolved: spi: spi-fsl-dspi: Fix crash when not using GPIO chip select Add check for the return value of spi_get_csgpiod() to avoid passing a NULL pointer to gpiod_direction_output(), preventing a crash when GPIO chip select is not used. Fix below crash: [4.251960] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 [4.260762] Mem abort info: [4.263556] ESR = 0x0000000096000004 [4.267308] EC = 0x25: DABT (current EL), IL = 32 bits [4.272624] SET = 0, FnV = 0 [4.275681] EA = 0, S1PTW = 0 [4.278822] FSC = 0x04: level 0 translation fault [4.283704] Data abort info: [4.286583] ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 [4.292074] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [4.297130] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [4.302445] [0000000000000000] user address but active_mm is swapper [4.308805] Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP [4.315072] Modules linked in: [4.318124] CPU: 2 UID: 0 PID: 1 Comm: swapper/0 Not tainted 6.12.0-rc4-next-20241023-00008-ga20ec42c5fc1 #359 [4.328130] Hardware name: LS1046A QDS Board (DT) [4.332832] pstate: 40000005 (nZcv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [4.339794] pc : gpiod_direction_output+0x34/0x5c [4.344505] lr : gpiod_direction_output+0x18/0x5c [4.349208] sp : ffff80008003b8f0 [4.352517] x29: ffff80008003b8f0 x28: 0000000000000000 x27: ffffc96bcc7e9068 [4.359659] x26: ffffc96bcc6e00b0 x25: ffffc96bcc598398 x24: ffff447400132810 [4.366800] x23: 0000000000000000 x22: 0000000011e1a300 x21: 0000000000020002 [4.373940] x20: 0000000000000000 x19: 0000000000000000 x18: ffffffffffffffff [4.381081] x17: ffff44740016e600 x16: 0000000500000003 x15: 0000000000000007 [4.388221] x14: 0000000000989680 x13: 0000000000020000 x12: 000000000000001e [4.395362] x11: 0044b82fa09b5a53 x10: 0000000000000019 x9 : 0000000000000008 [4.402502] x8 : 0000000000000002 x7 : 0000000000000007 x6 : 0000000000000000 [4.409641] x5 : 0000000000000200 x4 : 0000000002000000 x3 : 0000000000000000 [4.416781] x2 : 0000000000022202 x1 : 0000000000000000 x0 : 0000000000000000 [4.423921] Call trace: [4.426362] gpiod_direction_output+0x34/0x5c (P) [4.431067] gpiod_direction_output+0x18/0x5c (L) [4.435771] dspi_setup+0x220/0x334	5.5	More Details
CVE-2024-50160	In the Linux kernel, the following vulnerability has been resolved: ALSA: hda/cs8409: Fix possible NULL dereference If snd_hda_gen_add_kctl fails to allocate memory and returns NULL, then NULL pointer dereference will occur in the next line. Since dolphin_fixups function is a hda_fixup function which is not supposed to return any errors, add simple check before dereference, ignore the fail. Found by Linux Verification Center (linuxtesting.org) with SVACE.	5.5	More Details
CVE-2024-50161	In the Linux kernel, the following vulnerability has been resolved: bpf: Check the remaining info_cnt before repeating btf fields When trying to repeat the btf fields for array of nested struct, it doesn't check the remaining info_cnt. The following splat will be reported when the value of ret * nelems is greater than BTF_FIELDS_MAX: ------------[cut here]------------ UBSAN: array-index-out-of-bounds in ../kernel/bpf/btf.c:3951:49 index 11 is out of range for type 'btf_field_info [11]' CPU: 6 UID: 0 PID: 411 Comm: test_progs ..... 6.11.0-rc4+ #1 Tainted: [O]=OOT_MODULE Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS ... Call Trace: <TASK> dump_stack_lvl+0x57/0x70 dump_stack+0x10/0x20 ubsan_epilogue+0x9/0x40 __ubsan_handle_out_of_bounds+0x6f/0x80 ? kallsyms_lookup_name+0x48/0xb0 btf_parse_fields+0x992/0xce0 map_create+0x591/0x770 __sys_bpf+0x229/0x2410 __x64_sys_bpf+0x1f/0x30 x64_sys_call+0x199/0x9f0 do_syscall_64+0x3b/0xc0 entry_SYSCALL_64_after_hwframe+0x4b/0x53 RIP: 0033:0x7fea56f2cc5d ..... </TASK> ---[end trace]--- Fix it by checking the remaining info_cnt in btf_repeat_fields() before repeating the btf fields.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50225	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix error propagation of split bios The purpose of btrfs_bbio_propagate_error() shall be propagating an error of split bio to its original btrfs_bio, and tell the error to the upper layer. However, it's not working well on some cases. * Case 1. Immediate (or quick) end_bio with an error When btrfs sends btrfs_bio to mirrored devices, btrfs calls btrfs_bio_end_io() when all the mirroring bios are completed. If that btrfs_bio was split, it is from btrfs_clone_bioset and its end_io function is btrfs_orig_write_end_io. For this case, btrfs_bbio_propagate_error() accesses the orig_bbio's bio context to increase the error count. That works well in most cases. However, if the end_io is called enough fast, orig_bbio's (remaining part after split) bio context may not be properly set at that time. Since the bio context is set when the orig_bbio (the last btrfs_bio) is sent to devices, that might be too late for earlier split btrfs_bio's completion. That will result in NULL pointer dereference. That bug is easily reproducible by running btrfs/146 on zoned devices [1] and it shows the following trace. [1] You need raid-stripe-tree feature as it create "-d raid0 -m raid1" FS. BUG: kernel NULL pointer dereference, address: 0000000000000020 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: Oops: 0000 [#1] PREEMPT SMP PTI CPU: 1 UID: 0 PID: 13 Comm: kworker/u32:1 Not tainted 6.11.0-rc7-BTRFS-ZNS+ #474 Hardware name: Bochs Bochs, BIOS Bochs 01/01/2011 Workqueue: writeback wb_workfn (flush-btrfs-5) RIP: 0010:btrfs_bio_end_io+0xae/0xc0 [btrfs] BTRFS error (device dm-0): bdev /dev/mapper/error-test errs: wr 2, rd 0, flush 0, corrupt 0, gen 0 RSP: 0018:ffffc9000006f248 EFLAGS: 00010246 RAX: 0000000000000000 RBX: ffff888005a7f080 RCX: ffffc9000006f1dc RDX: 0000000000000000 RSI: 000000000000000a RDI: ffff888005a7f080 RBP: ffff888011dfc540 R08: 0000000000000000 R09: 0000000000000001 R10: ffffffff82e508e0 R11: 0000000000000005 R12: ffff88800ddfbe58 R13: ffff888005a7f080 R14: ffff888005a7f158 R15: ffff888005a7f158 FS: 0000000000000000(0000) GS:ffff88803ea80000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000020 CR3: 0000000002e22006 CR4: 0000000000370ef0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> ? __die_body.cold+0x19/0x26 ? page_fault_oops+0x13e/0x2b0 ? _printk+0x58/0x73 ? do_user_addr_fault+0x5f/0x750 ? exc_page_fault+0x76/0x240 ? asm_exc_page_fault+0x22/0x30 ? btrfs_bio_end_io+0xae/0xc0 [btrfs] ? btrfs_log_dev_io_error+0x7f/0x90 [btrfs] btrfs_orig_write_end_io+0x51/0x90 [btrfs] dm_submit_bio+0x5c2/0xa50 [dm_mod] ? find_held_lock+0x2b/0x80 ? blk_try_enter_queue+0x90/0x1e0 __submit_bio+0xe0/0x130 ? ktime_get+0x10a/0x160 ? lockdep_hardirqs_on+0x74/0x100 submit_bio_noacct_nocheck+0x199/0x410 btrfs_submit_bio+0x7d/0x150 [btrfs] btrfs_submit_chunk+0x1a1/0x6d0 [btrfs] ? lockdep_hardirqs_on+0x74/0x100 ? __folio_start_writeback+0x10/0x2c0 btrfs_submit_bbio+0x1c/0x40 [btrfs] submit_one_bio+0x44/0x60 [btrfs] submit_extent_folio+0x13f/0x330 [btrfs] ? btrfs_set_range_writeback+0xa3/0xd0 [btrfs] extent_writepage_io+0x18b/0x360 [btrfs] extent_write_locked_range+0x17c/0x340 [btrfs] ? __pfx_end_bbio_data_write+0x10/0x10 [btrfs] run_delalloc_cow+0x71/0xd0 [btrfs] btrfs_run_delalloc_range+0x176/0x500 [btrfs] ? find_lock_delalloc_range+0x119/0x260 [btrfs] writepage_delalloc+0x2ab/0x480 [btrfs] extent_write_cache_pages+0x236/0x7d0 [btrfs] btrfs_writepages+0x72/0x130 [btrfs] do_writepages+0xd4/0x240 ? find_held_lock+0x2b/0x80 ? wbc_attach_and_unlock_inode+0x12c/0x290 ? wbc_attach_and_unlock_inode+0x12c/0x29 ---truncated---	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50223	In the Linux kernel, the following vulnerability has been resolved: sched/numa: Fix the potential null pointer dereference in task_numa_work() When running stress-ng-vm-segv test, we found a null pointer dereference error in task_numa_work(). Here is the backtrace: [323676.066985] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000020 ..... [323676.067108] CPU: 35 PID: 2694524 Comm: stress-ng-vm-se ..... [323676.067113] pstate: 23401009 (nzCv daif +PAN -UAO +TCO +DIT +SSBS BTYPE=--) [323676.067115] pc : vma_migratable+0x1c/0xd0 [323676.067122] lr : task_numa_work+0x1ec/0x4e0 [323676.067127] sp : ffff8000ada73d20 [323676.067128] x29: ffff8000ada73d20 x28: 0000000000000000 x27: 000000003e89f010 [323676.067130] x26: 0000000000080000 x25: ffff800081b5c0d8 x24: ffff800081b27000 [323676.067133] x23: 0000000000010000 x22: 0000000104d18cc0 x21: ffff0009f7158000 [323676.067135] x20: 0000000000000000 x19: 0000000000000000 x18: ffff8000ada73db8 [323676.067138] x17: 0001400000000000 x16: ffff800080df40b0 x15: 0000000000000035 [323676.067140] x14: ffff8000ada73cc8 x13: 1fffe0017cc72001 x12: ffff8000ada73cc8 [323676.067142] x11: ffff80008001160c x10: ffff000be639000c x9 : ffff8000800f4ba4 [323676.067145] x8 : ffff000810375000 x7 : ffff8000ada73974 x6 : 0000000000000001 [323676.067147] x5 : 0068000b33e26707 x4 : 0000000000000001 x3 : ffff0009f7158000 [323676.067149] x2 : 0000000000000041 x1 : 0000000000004400 x0 : 0000000000000000 [323676.067152] Call trace: [323676.067153] vma_migratable+0x1c/0xd0 [323676.067155] task_numa_work+0x1ec/0x4e0 [323676.067157] task_work_run+0x78/0xd8 [323676.067161] do_notify_resume+0x1ec/0x290 [323676.067163] el0_svc+0x150/0x160 [323676.067167] el0t_64_sync_handler+0xf8/0x128 [323676.067170] el0t_64_sync+0x17c/0x180 [323676.067173] Code: d2888001 910003fd f9000bf3 aa0003f3 (f9401000) [323676.067177] SMP: stopping secondary CPUs [323676.070184] Starting crashdump kernel... stress-ng-vm-segv in stress-ng is used to stress test the SIGSEGV error handling function of the system, which tries to cause a SIGSEGV error on return from unmapping the whole address space of the child process. Normally this program will not cause kernel crashes. But before the munmap system call returns to user mode, a potential task_numa_work() for numa balancing could be added and executed. In this scenario, since the child process has no vma after munmap, the vma_next() in task_numa_work() will return a null pointer even if the vma iterator restarts from 0. Recheck the vma pointer before dereferencing it in task_numa_work().	5.5	More Details
CVE-2024-50156	In the Linux kernel, the following vulnerability has been resolved: drm/msm: Avoid NULL dereference in msm_disp_state_print_regs() If the allocation in msm_disp_state_dump_regs() failed then `block->state` can be NULL. The msm_disp_state_print_regs() function _does_ have code to try to handle it with: if (*reg) dump_addr = *reg; ...but since "dump_addr" is initialized to NULL the above is actually a noop. The code then goes on to dereference `dump_addr`. Make the function print "Registers not stored" when it sees a NULL to solve this. Since we're touching the code, fix msm_disp_state_print_regs() not to pointlessly take a double-pointer and properly mark the pointer as `const`. Patchwork: https://patchwork.freedesktop.org/patch/619657/	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50162	In the Linux kernel, the following vulnerability has been resolved: bpf: devmap: provide rxq after redirect rxq contains a pointer to the device from where the redirect happened. Currently, the BPF program that was executed after a redirect via BPF_MAP_TYPE_DEVMAP* does not have it set. This is particularly bad since accessing ingress_ifindex, e.g. SEC("xdp") int prog(struct xdp_md *pkt) { return bpf_redirect_map(&dev_redirect_map, 0, 0); } SEC("xdp/devmap") int prog_after_redirect(struct xdp_md *pkt) { bpf_printk("ifindex %i", pkt->ingress_ifindex); return XDP_PASS; } depends on access to rxq, so a NULL pointer gets dereferenced: <1>[574.475170] BUG: kernel NULL pointer dereference, address: 0000000000000000 <1>[574.475188] #PF: supervisor read access in kernel mode <1>[574.475194] #PF: error_code(0x0000) - not-present page <6>[574.475199] PGD 0 P4D 0 <4>[574.475207] Oops: Oops: 0000 [#1] PREEMPT SMP NOPTI <4>[574.475217] CPU: 4 UID: 0 PID: 217 Comm: kworker/4:1 Not tainted 6.11.0-rc5-reduced-00859-g780801200300 #23 <4>[574.475226] Hardware name: Intel(R) Client Systems NUC13ANHi7/NUC13ANBi7, BIOS ANRPL357.0026.2023.0314.1458 03/14/2023 <4>[574.475231] Workqueue: mld mld_ifc_work <4>[574.475247] RIP: 0010:bpf_prog_5e13354d9cf5018a_prog_after_redirect+0x17/0x3c <4>[574.475257] Code: cc cc cc cc cc cc cc 80 00 00 00 cc cc cc cc cc cc cc f3 0f 1e fa 0f 1f 44 00 00 66 90 55 48 89 e5 f3 0f 1e fa 48 8b 57 20 <48> 8b 52 00 8b 92 e0 00 00 00 48 bf f8 a6 d5 c4 5d a0 ff ff be 0b <4>[574.475263] RSP: 0018:ffffa62440280c98 EFLAGS: 00010206 <4>[574.475269] RAX: ffffa62440280cd8 RBX: 0000000000000001 RCX: 0000000000000000 <4>[574.475274] RDX: 0000000000000000 RSI: ffffa62440549048 RDI: ffffa62440280ce0 <4>[574.475278] RBP: ffffa62440280c98 R08: 0000000000000002 R09: 0000000000000001 <4>[574.475281] R10: ffffa05dc8b98000 R11: ffffa05f577fca40 R12: ffffa05dcab24000 <4>[574.475285] R13: ffffa62440280ce0 R14: ffffa62440549048 R15: ffffa62440549000 <4>[574.475289] FS: 0000000000000000(0000) GS:ffffa05f4f700000(0000) knlGS:0000000000000000 <4>[574.475294] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 <4>[574.475298] CR2: 0000000000000000 CR3: 000000025522e000 CR4: 0000000000f50ef0 <4>[574.475303] PKRU: 55555554 <4>[574.475306] Call Trace: <4>[574.475313] <IRQ> <4>[574.475318] ? __die+0x23/0x70 <4>[574.475329] ? page_fault_oops+0x180/0x4c0 <4>[574.475339] ? skb_pp_cow_data+0x34c/0x490 <4>[574.475346] ? kmem_cache_free+0x257/0x280 <4>[574.475357] ? exc_page_fault+0x67/0x150 <4>[574.475368] ? asm_exc_page_fault+0x26/0x30 <4>[574.475381] ? bpf_prog_5e13354d9cf5018a_prog_after_redirect+0x17/0x3c <4>[574.475386] bq_xmit_all+0x158/0x420 <4>[574.475397] __dev_flush+0x30/0x90 <4>[574.475407] veth_poll+0x216/0x250 [veth] <4>[574.475421] __napi_poll+0x28/0x1c0 <4>[574.475430] net_rx_action+0x32d/0x3a0 <4>[574.475441] handle_softirqs+0xcb/0x2c0 <4>[574.475451] do_softirq+0x40/0x60 <4>[574.475458] </IRQ> <4>[574.475461] <TASK> <4>[574.475464] __local_bh_enable_ip+0x66/0x70 <4>[574.475471] __dev_queue_xmit+0x268/0xe40 <4>[574.475480] ? selinux_ip_postroute+0x213/0x420 <4>[574.475491] ? alloc_skb_with_frags+0x4a/0x1d0 <4>[574.475502] ip6_finish_output2+0x2be/0x640 <4>[574.475512] ? nf_hook_slow+0x42/0xf0 <4>[574.475521] ip6_finish_output+0x194/0x300 <4>[574.475529] ? __pfx_ip6_finish_output+0x10/0x10 <4>[574.475538] mld_sendpack+0x17c/0x240 <4>[574.475548] mld_ifc_work+0x192/0x410 <4>[574.475557] process_one_work+0x15d/0x380 <4>[574.475566] worker_thread+0x29d/0x3a0 <4>[574.475573] ? __pfx_worker_thread+0x10/0x10 <4>[574.475580] ? __pfx_worker_thread+0x10/0x10 <4>[574.475587] kthread+0xcd/0x100 <4>[574.475597] ? __pfx_kthread+0x10/0x10 <4>[574.475606] ret_from_fork+0x31/0x50 <4>[574.475615] ? __pfx_kthread+0x10/0x10 <4>[574.475623] ret_from_fork_asm+0x1a/0x ---truncated---	5.5	More Details
CVE-2024-50163	In the Linux kernel, the following vulnerability has been resolved: bpf: Make sure internal and UAPI bpf_redirect flags don't overlap The bpf_redirect_info is shared between the SKB and XDP redirect paths, and the two paths use the same numeric flag values in the ri->flags field (specifically, BPF_F_BROADCAST == BPF_F_NEXTHOP). This means that if skb bpf_redirect_neigh() is used with a non-NULL params argument and, subsequently, an XDP redirect is performed using the same bpf_redirect_info struct, the XDP path will get confused and end up crashing, which syzbot managed to trigger. With the stack-allocated bpf_redirect_info, the structure is no longer shared between the SKB and XDP paths, so the crash doesn't happen anymore. However, different code paths using identically-numbered flag values in the same struct field still seems like a bit of a mess, so this patch cleans that up by moving the flag definitions together and redefining the three flags in BPF_F_REDIRECT_INTERNAL to not overlap with the flags used for XDP. It also adds a BUILD_BUG_ON() check to make sure the overlap is not re-introduced by mistake.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50165	In the Linux kernel, the following vulnerability has been resolved: bpf: Preserve param->string when parsing mount options In bpf_parse_param(), keep the value of param->string intact so it can be freed later. Otherwise, the kmalloc area pointed to by param->string will be leaked as shown below: unreferenced object 0xffff888118c46d20 (size 8): comm "new_name", pid 12109, jiffies 4295580214 hex dump (first 8 bytes): 61 6e 79 00 38 c9 5c 7e any.8.\~ backtrace (crc e1b7f876): [<00000000c6848ac7>] kmemleak_alloc+0x4b/0x80 [<00000000de9f7d00>] __kmalloc_node_track_caller_noprof+0x36e/0x4a0 [<000000003e29b886>] memdup_user+0x32/0xa0 [<0000000007248326>] strndup_user+0x46/0x60 [<0000000035b3dd29>] __x64_sys_fsconfig+0x368/0x3d0 [<0000000018657927>] x64_sys_call+0xff/0x9f0 [<00000000c0cabc95>] do_syscall_64+0x3b/0xc0 [<000000002f331597>] entry_SYSCALL_64_after_hwframe+0x4b/0x53	5.5	More Details
CVE-2024-50166	In the Linux kernel, the following vulnerability has been resolved: fsl/fman: Fix refcount handling of fman-related devices In mac_probe() there are multiple calls to of_find_device_by_node(), fman_bind() and fman_port_bind() which takes references to of_dev->dev. Not all references taken by these calls are released later on error path in mac_probe() and in mac_remove() which lead to reference leaks. Add references release.	5.5	More Details
CVE-2024-50167	In the Linux kernel, the following vulnerability has been resolved: be2net: fix potential memory leak in be_xmit() The be_xmit() returns NETDEV_TX_OK without freeing skb in case of be_xmit_enqueue() fails, add dev_kfree_skb_any() to fix it.	5.5	More Details
CVE-2024-50168	In the Linux kernel, the following vulnerability has been resolved: net/sun3_82586: fix potential memory leak in sun3_82586_send_packet() The sun3_82586_send_packet() returns NETDEV_TX_OK without freeing skb in case of skb->len being too long, add dev_kfree_skb() to fix it.	5.5	More Details
CVE-2024-50169	In the Linux kernel, the following vulnerability has been resolved: vsock: Update rx_bytes on read_skb() Make sure virtio_transport_inc_rx_pkt() and virtio_transport_dec_rx_pkt() calls are balanced (i.e. virtio_vsock_sock::rx_bytes doesn't lie) after vsock_transport::read_skb(). While here, also inform the peer that we've freed up space and it has more credit. Failing to update rx_bytes after packet is dequeued leads to a warning on SOCK_STREAM recv(): [233.396654] rx_queue is empty, but rx_bytes is non-zero [233.396702] WARNING: CPU: 11 PID: 40601 at net/vmw_vsock/virtio_transport_common.c:589	5.5	More Details
CVE-2024-50157	In the Linux kernel, the following vulnerability has been resolved: RDMA/bnxt_re: Avoid CPU lockups due fifo occupancy check loop Driver waits indefinitely for the fifo occupancy to go below a threshold as soon as the pacing interrupt is received. This can cause soft lockup on one of the processors, if the rate of DB is very high. Add a loop count for FPGA and exit the __wait_for_fifo_occupancy_below_th if the loop is taking more time. Pacing will be continuing until the occupancy is below the threshold. This is ensured by the checks in bnxt_re_pacing_timer_exp and further scheduling the work for pacing based on the fifo occupancy.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50231	In the Linux kernel, the following vulnerability has been resolved: iio: gts-helper: Fix memory leaks in iio_gts_build_avail_scale_table() modprobe iio-test-gts and rmmod it, then the following memory leak occurs: unreferenced object 0xffffff80c810be00 (size 64): comm "kunit_try_catch", pid 1654, jiffies 4294913981 hex dump (first 32 bytes): 02 00 00 00 08 00 00 00 20 00 00 00 40 00 00 00 ....@... 80 00 00 00 00 02 00 00 00 00 04 00 00 00 08 00 00 ..... backtrace (crc a63d875e): [<0000000028c1b3c2>] kmemleak_alloc+0x34/0x40 [<000000001d6ecc87>] __kmalloc_noprof+0x2bc/0x3c0 [<00000000393795c1>] devm_iio_init_iio_gts+0x4b4/0x16f4 [<0000000071bb4b09>] 0xffffffdf052a62e0 [<000000000315bc18>] 0xffffffdf052a6488 [<00000000f9dc55b5>] kunit_try_run_case+0x13c/0x3ac [<00000000175a3fd4>] kunit_generic_run_threadfn_adapter+0x80/0xec [<00000000f505065d>] kthread+0x2e8/0x374 [<00000000bbfb0e5d>] ret_from_fork+0x10/0x20 unreferenced object 0xffffff80cbfe9e70 (size 16): comm "kunit_try_catch", pid 1658, jiffies 4294914015 hex dump (first 16 bytes): 10 00 00 00 40 00 00 00 80 00 00 00 00 00 00 00 ....@..... backtrace (crc 857f0cb4): [<0000000028c1b3c2>] kmemleak_alloc+0x34/0x40 [<000000001d6ecc87>] __kmalloc_noprof+0x2bc/0x3c0 [<00000000393795c1>] devm_iio_init_iio_gts+0x4b4/0x16f4 [<0000000071bb4b09>] 0xffffffdf052a62e0 [<000000007d089d45>] 0xffffffdf052a6864 [<00000000f9dc55b5>] kunit_try_run_case+0x13c/0x3ac [<00000000175a3fd4>] kunit_generic_run_threadfn_adapter+0x80/0xec [<00000000f505065d>] kthread+0x2e8/0x374 [<00000000bbfb0e5d>] ret_from_fork+0x10/0x20 ..... It includes 5*5 times "size 64" memory leaks, which correspond to 5 times test_init_iio_gain_scale() calls with gts_test_gains size 10 (10*size(int)) and gts_test_itimes size 5. It also includes 5*1 times "size 16" memory leak, which correspond to one time __test_init_iio_gain_scale() call with gts_test_gains_gain_low size 3 (3*size(int)) and gts_test_itimes size 5. The reason is that the per_time_gains[i] is not freed which is allocated in the "gts->num_itime" for loop in iio_gts_build_avail_scale_table().	5.5	More Details
CVE-2024-50229	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix potential deadlock with newly created symlinks Syzbot reported that page_symlink(), called by nilfs_symlink(), triggers memory reclamation involving the filesystem layer, which can result in circular lock dependencies among the reader/writer semaphore nilfs->ns_segctor_sem, s_writers percpu_rwsem (intwrite) and the fs_reclaim pseudo lock. This is because after commit 21fc61c73c39 ("don't put symlink bodies in pagecache into highmem"), the gfp flags of the page cache for symbolic links are overwritten to GFP_KERNEL via inode_nohighmem(). This is not a problem for symlinks read from the backing device, because the __GFP_FS flag is dropped after inode_nohighmem() is called. However, when a new symlink is created with nilfs_symlink(), the gfp flags remain overwritten to GFP_KERNEL. Then, memory allocation called from page_symlink() etc. triggers memory reclamation including the FS layer, which may call nilfs_evict_inode() or nilfs_dirty_inode(). And these can cause a deadlock if they are called while nilfs->ns_segctor_sem is held: Fix this issue by dropping the __GFP_FS flag from the page cache GFP flags of newly created symlinks in the same way that nilfs_new_inode() and __nilfs_read_inode() do, as a workaround until we adopt nofs allocation scope consistently or improve the locking constraints.	5.5	More Details
CVE-2024-50171	In the Linux kernel, the following vulnerability has been resolved: net: systemport: fix potential memory leak in bcm_sysport_xmit() The bcm_sysport_xmit() returns NETDEV_TX_OK without freeing skb in case of dma_map_single() fails, add dev_kfree_skb() to fix it.	5.5	More Details
CVE-2024-50244	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: Additional check in ni_clear() Checking of NTFS_FLAGS_LOG_REPLAYING added to prevent access to uninitialized bitmap during replay process.	5.5	More Details
CVE-2024-50243	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: Fix general protection fault in run_is_mapped_full Fixed deleating of a non-resident attribute in ntfs_create_inode() rollback.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50147	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix command bitmask initialization Command bitmask have a dedicated bit for MANAGE_PAGES command, this bit isn't Initialize during command bitmask Initialization, only during MANAGE_PAGES. In addition, mlx5_cmd_trigger_completions() is trying to trigger completion for MANAGE_PAGES command as well. Hence, in case health error occurred before any MANAGE_PAGES command have been invoke (for example, during mlx5_enable_hca()), mlx5_cmd_trigger_completions() will try to trigger completion for MANAGE_PAGES command, which will result in null-ptr-deref error.[1] Fix it by Initialize command bitmask correctly. While at it, re-write the code for better understanding. [1] BUG: KASAN: null-ptr-deref in mlx5_cmd_trigger_completions+0x1db/0x600 [mlx5_core] Write of size 4 at addr 0000000000000214 by task kworker/u96:2/12078 CPU: 10 PID: 12078 Comm: kworker/u96:2 Not tainted 6.9.0-rc2_for_upstream_debug_2024_04_07_19_01 #1 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.13.0-0-gf21b5a4aeb02-prebuilt.qemu.org 04/01/2014 Workqueue: mlx5_health0000:08:00.0 mlx5_fw_fatal_reporter_err_work [mlx5_core] Call Trace: <TASK> dump_stack_lvl+0x7e/0xc0 kasan_report+0xb9/0xf0 kasan_check_range+0xec/0x190 mlx5_cmd_trigger_completions+0x1db/0x600 [mlx5_core] mlx5_cmd_flush+0x94/0x240 [mlx5_core] enter_error_state+0x6c/0xd0 [mlx5_core] mlx5_fw_fatal_reporter_err_work+0xf3/0x480 [mlx5_core] process_one_work+0x787/0x1490 ? lockdep_hardirqs_on_prepare+0x400/0x400 ? pwq_dec_nr_in_flight+0xda0/0xda0 ? assign_work+0x168/0x240 worker_thread+0x586/0xd30 ? rescuer_thread+0xae0/0xae0 kthread+0x2df/0x3b0 ? kthread_complete_and_exit+0x20/0x20 ret_from_fork+0x2d/0x70 ? kthread_complete_and_exit+0x20/0x20 ret_from_fork_asm+0x11/0x20 </TASK>	5.5	More Details
CVE-2024-50241	In the Linux kernel, the following vulnerability has been resolved: NFSD: Initialize struct nfsd4_copy earlier Ensure the refcount and async_copies fields are initialized early. cleanup_async_copy() will reference these fields if an error occurs in nfsd4_copy(). If they are not correctly initialized, at the very least, a refcount underflow occurs.	5.5	More Details
CVE-2024-50148	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: bnep: fix wild-memory-access in proto_unregister There's issue as follows: KASAN: maybe wild-memory-access in range [0xdead...108-0xdead...10f] CPU: 3 UID: 0 PID: 2805 Comm: rmmod Tainted: G W RIP: 0010:proto_unregister+0xee/0x400 Call Trace: <TASK> __do_sys_delete_module+0x318/0x580 do_syscall_64+0xc1/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f As bnep_init() ignore bnep_sock_init()'s return value, and bnep_sock_init() will cleanup all resource. Then when remove bnep module will call bnep_sock_cleanup() to cleanup sock's resource. To solve above issue just return bnep_sock_init()'s return value in bnep_exit().	5.5	More Details
CVE-2024-50240	In the Linux kernel, the following vulnerability has been resolved: phy: qcom: qmp-usb: fix NULL-deref on runtime suspend Commit 413db06c05e7 ("phy: qcom-qmp-usb: clean up probe initialisation") removed most users of the platform device driver data, but mistakenly also removed the initialisation despite the data still being used in the runtime PM callbacks. Restore the driver data initialisation at probe to avoid a NULL-pointer dereference on runtime suspend. Apparently no one uses runtime PM, which currently needs to be enabled manually through sysfs, with this driver.	5.5	More Details
CVE-2024-50149	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Don't free job in TDR Freeing job in TDR is not safe as TDR can pass the run_job thread resulting in UAF. It is only safe for free job to naturally be called by the scheduler. Rather free job in TDR, add to pending list. (cherry picked from commit ea2f6a77d0c40d97f4a4dc93fee4afe15d94926d)	5.5	More Details
CVE-2024-50239	In the Linux kernel, the following vulnerability has been resolved: phy: qcom: qmp-usb-legacy: fix NULL-deref on runtime suspend Commit 413db06c05e7 ("phy: qcom-qmp-usb: clean up probe initialisation") removed most users of the platform device driver data from the qcom-qmp-usb driver, but mistakenly also removed the initialisation despite the data still being used in the runtime PM callbacks. This bug was later reproduced when the driver was copied to create the qmp-usb-legacy driver. Restore the driver data initialisation at probe to avoid a NULL-pointer dereference on runtime suspend. Apparently no one uses runtime PM, which currently needs to be enabled manually through sysfs, with these drivers.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50238	In the Linux kernel, the following vulnerability has been resolved: phy: qcom: qmp-usbc: fix NULL-deref on runtime suspend Commit 413db06c05e7 ("phy: qcom-qmp-usb: clean up probe initialisation") removed most users of the platform device driver data from the qcom-qmp-usb driver, but mistakenly also removed the initialisation despite the data still being used in the runtime PM callbacks. This bug was later reproduced when the driver was copied to create the qmp-usbc driver. Restore the driver data initialisation at probe to avoid a NULL-pointer dereference on runtime suspend. Apparently no one uses runtime PM, which currently needs to be enabled manually through sysfs, with these drivers.	5.5	More Details
CVE-2024-50237	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: do not pass a stopped vif to the driver in .get_txpower Avoid potentially crashing in the driver because of uninitialized private data	5.5	More Details
CVE-2024-50152	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix possible double free in smb2_set_ea() Clang static checker(scan-build) warning： fs/smb/client/smb2ops.c:1304:2: Attempt to free released memory. 1304	kfree(ea);	^~~~~~~~ There is a double free in such case: 'ea is initialized to NULL' -> 'first successful memory allocation for ea' -> 'something failed, goto sea_exit' -> 'first memory release for ea' -> 'goto replay_again' -> 'second goto sea_exit before allocate memory for ea' -> 'second memory release for ea resulted in double free'. Re-initialie 'ea' to NULL near to the replay_again label, it can fix this double free problem.	5.5	More Details
CVE-2024-50236	In the Linux kernel, the following vulnerability has been resolved: wifi: ath10k: Fix memory leak in management tx In the current logic, memory is allocated for storing the MSDU context during management packet TX but this memory is not being freed during management TX completion. Similar leaks are seen in the management TX cleanup logic. Kmemleak reports this problem as below, unreferenced object 0xffffff80b64ed250 (size 16): comm "kworker/u16:7", pid 148, jiffies 4294687130 (age 714.199s) hex dump (first 16 bytes): 00 2b d8 d8 80 ff ff ff c4 74 e9 fd 07 00 00 00 .+.....t..... backtrace: [<ffffffe6e7b245dc>] __kmem_cache_alloc_node+0x1e4/0x2d8 [<ffffffe6e7adde88>] kmalloc_trace+0x48/0x110 [<ffffffe6bbd765fc>] ath10k_wmi_tlv_op_gen_mgmt_tx_send+0xd4/0x1d8 [ath10k_core] [<ffffffe6bbd3eed4>] ath10k_mgmt_over_wmi_tx_work+0x134/0x298 [ath10k_core] [<ffffffe6e78d5974>] process_scheduled_works+0x1ac/0x400 [<ffffffe6e78d60b8>] worker_thread+0x208/0x328 [<ffffffe6e78dc890>] kthread+0x100/0x1c0 [<ffffffe6e78166c0>] ret_from_fork+0x10/0x20 Free the memory during completion and cleanup to fix the leak. Protect the mgmt_pending_tx idr_remove() operation in ath10k_wmi_tlv_op_cleanup_mgmt_tx_send() using ar->data_lock similar to other instances. Tested-on: WCN3990 hw1.0 SNOC WLAN.HL.2.0-01387-QCAHLSWMTPLZ-1	5.5	More Details
CVE-2024-50233	In the Linux kernel, the following vulnerability has been resolved: staging: iio: frequency: ad9832: fix division by zero in ad9832_calc_freqreg() In the ad9832_write_frequency() function, clk_get_rate() might return 0. This can lead to a division by zero when calling ad9832_calc_freqreg(). The check if (fout > (clk_get_rate(st->mclk) / 2)) does not protect against the case when fout is 0. The ad9832_write_frequency() function is called from ad9832_write(), and fout is derived from a text buffer, which can contain any value.	5.5	More Details
CVE-2024-50232	In the Linux kernel, the following vulnerability has been resolved: iio: adc: ad7124: fix division by zero in ad7124_set_channel_odr() In the ad7124_write_raw() function, parameter val can potentially be zero. This may lead to a division by zero when DIV_ROUND_CLOSEST() is called within ad7124_set_channel_odr(). The ad7124_write_raw() function is invoked through the sequence: iio_write_channel_raw() -> iio_write_channel_attribute() -> iio_channel_write(), with no checks in place to ensure val is non-zero.	5.5	More Details
CVE-2024-50153	In the Linux kernel, the following vulnerability has been resolved: scsi: target: core: Fix null-ptr-deref in target_alloc_device() There is a null-ptr-deref issue reported by KASAN: BUG: KASAN: null-ptr-deref in target_alloc_device+0xbc4/0xbe0 [target_core_mod] ... kasan_report+0xb9/0xf0 target_alloc_device+0xbc4/0xbe0 [target_core_mod] core_dev_setup_virtual_lun0+0xef/0x1f0 [target_core_mod] target_core_init_configfs+0x205/0x420 [target_core_mod] do_one_initcall+0xdd/0x4e0 ... entry_SYSCALL_64_after_hwframe+0x76/0x7e In target_alloc_device(), if allocing memory for dev queues fails, then dev will be freed by dev->transport->free_device(), but dev->transport is not initialized at that time, which will lead to a null pointer reference problem. Fixing this bug by freeing dev with hba->backend->ops->free_device().	5.5	More Details
CVE-2024-50170	In the Linux kernel, the following vulnerability has been resolved: net: bcmasp: fix potential memory leak in bcmasp_xmit() The bcmasp_xmit() returns NETDEV_TX_OK without freeing skb in case of mapping fails, add dev_kfree_skb() to fix it.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50214	In the Linux kernel, the following vulnerability has been resolved: drm/connector: hdmi: Fix memory leak in drm_display_mode_from_cea_vic() modprobe drm_connector_test and then rmmod drm_connector_test, the following memory leak occurs. The `mode` allocated in drm_mode_duplicate() called by drm_display_mode_from_cea_vic() is not freed, which cause the memory leak: unreferenced object 0xffffff80cb0ee400 (size 128): comm "kunit_try_catch", pid 1948, jiffies 4294950339 hex dump (first 32 bytes): 14 44 02 00 80 07 d8 07 04 08 98 08 00 00 38 04 .D.....8. 3c 04 41 04 65 04 00 00 05 00 00 00 00 00 00 00 <.A.e..... backtrace (crc 90e9585c): [<00000000ec42e3d7>] kmemleak_alloc+0x34/0x40 [<00000000d0ef055a>] __kmalloc_cache_noprof+0x26c/0x2f4 [<00000000c2062161>] drm_mode_duplicate+0x44/0x19c [<00000000f96c74aa>] drm_display_mode_from_cea_vic+0x88/0x98 [<00000000d8f2c8b4>] 0xffffffdc982a4868 [<000000005d164dbc>] kunit_try_run_case+0x13c/0x3ac [<000000006fb23398>] kunit_generic_run_threadfn_adapter+0x80/0xec [<000000006ea56ca0>] kthread+0x2e8/0x374 [<000000000676063f>] ret_from_fork+0x10/0x20 ..... Free `mode` by using drm_kunit_display_mode_from_cea_vic() to fix it.	5.5	More Details
CVE-2024-50146	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Don't call cleanup on profile rollback failure When profile rollback fails in mlx5e_netdev_change_profile, the netdev profile var is left set to NULL. Avoid a crash when unloading the driver by not calling profile->cleanup in such a case. This was encountered while testing, with the original trigger that the wq rescuer thread creation got interrupted (presumably due to Ctrl+C-ing modprobe), which gets converted to ENOMEM (-12) by mlx5e_priv_init, the profile rollback also fails for the same reason (signal still active) so the profile is left as NULL, leading to a crash later in _mlx5e_remove. [732.473932] mlx5_core 0000:08:00.1: E-Switch: Unload vfs: mode(OFFLOADS), nvfs(2), necvfs(0), active vports(2) [734.525513] workqueue: Failed to create a rescuer kthread for wq "mlx5e": -EINTR [734.557372] mlx5_core 0000:08:00.1: mlx5e_netdev_init_profile:6235:(pid 6086): mlx5e_priv_init failed, err=-12 [734.559187] mlx5_core 0000:08:00.1 eth3: mlx5e_netdev_change_profile: new profile init failed, -12 [734.560153] workqueue: Failed to create a rescuer kthread for wq "mlx5e": -EINTR [734.589378] mlx5_core 0000:08:00.1: mlx5e_netdev_init_profile:6235:(pid 6086): mlx5e_priv_init failed, err=-12 [734.591136] mlx5_core 0000:08:00.1 eth3: mlx5e_netdev_change_profile: failed to rollback to orig profile, -12 [745.537492] BUG: kernel NULL pointer dereference, address: 0000000000000008 [745.538222] #PF: supervisor read access in kernel mode <snipped> [745.551290] Call Trace: [745.551590] <TASK> [745.551866] ? __die+0x20/0x60 [745.552218] ? page_fault_oops+0x150/0x400 [745.555307] ? exc_page_fault+0x79/0x240 [745.555729] ? asm_exc_page_fault+0x22/0x30 [745.556166] ? mlx5e_remove+0x6b/0xb0 [mlx5_core] [745.556698] auxiliary_bus_remove+0x18/0x30 [745.557134] device_release_driver_internal+0x1df/0x240 [745.557654] bus_remove_device+0xd7/0x140 [745.558075] device_del+0x15b/0x3c0 [745.558456] mlx5_rescan_drivers_locked.part.0+0xb1/0x2f0 [mlx5_core] [745.559112] mlx5_unregister_device+0x34/0x50 [mlx5_core] [745.559686] mlx5_uninit_one+0x46/0xf0 [mlx5_core] [745.560203] remove_one+0x4e/0xd0 [mlx5_core] [745.560694] pci_device_remove+0x39/0xa0 [745.561112] device_release_driver_internal+0x1df/0x240 [745.561631] driver_detach+0x47/0x90 [745.562022] bus_remove_driver+0x84/0x100 [745.562444] pci_unregister_driver+0x3b/0x90 [745.562890] mlx5_cleanup+0xc/0x1b [mlx5_core] [745.563415] __x64_sys_delete_module+0x14d/0x2f0 [745.563886] ? kmem_cache_free+0x1b0/0x460 [745.564313] ? lockdep_hardirqs_on_prepare+0xe2/0x190 [745.564825] do_syscall_64+0x6d/0x140 [745.565223] entry_SYSCALL_64_after_hwframe+0x4b/0x53 [745.565725] RIP: 0033:0x7f1579b1288b	5.5	More Details
CVE-2024-50205	In the Linux kernel, the following vulnerability has been resolved: ALSA: firewire-lib: Avoid division by zero in apply_constraint_to_size() The step variable is initialized to zero. It is changed in the loop, but if it's not changed it will remain zero. Add a variable check before the division. The observed behavior was introduced by commit 826b5de90c0b ("ALSA: firewire-lib: fix insufficient PCM rule for period/buffer size"), and it is difficult to show that any of the interval parameters will satisfy the snd_interval_test() condition with data from the amdtp_rate_table[] table. Found by Linux Verification Center (linuxtesting.org) with SVACE.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50195	In the Linux kernel, the following vulnerability has been resolved: posix-clock: Fix missing timespec64 check in pc_clock_settime() As Andrew pointed out, it will make sense that the PTP core checked timespec64 struct's tv_sec and tv_nsec range before calling ptp->info->settime64(). As the man manual of clock_settime() said, if tp.tv_sec is negative or tp.tv_nsec is outside the range [0..999,999,999], it should return EINVAL, which include dynamic clocks which handles PTP clock, and the condition is consistent with timespec64_valid(). As Thomas suggested, timespec64_valid() only check the timespec is valid, but not ensure that the time is in a valid range, so check it ahead using timespec64_valid_strict() in pc_clock_settime() and return -EINVAL if not valid. There are some drivers that use tp->tv_sec and tp->tv_nsec directly to write registers without validity checks and assume that the higher layer has checked it, which is dangerous and will benefit from this, such as hclge_ptp_settime(), igb_ptp_settime_i210(), _rcar_gen4_ptp_settime(), and some drivers can remove the checks of itself.	5.5	More Details
CVE-2024-50196	In the Linux kernel, the following vulnerability has been resolved: pinctrl: ocelot: fix system hang on level based interrupts The current implementation only calls chained_irq_enter() and chained_irq_exit() if it detects pending interrupts. ``` for (i = 0; i < info->stride; i++) { uregmap_read(info->map, id_reg + 4 * i, &reg); if (!reg) continue; chained_irq_enter(parent_chip, desc); ``` However, in case of GPIO pin configured in level mode and the parent controller configured in edge mode, GPIO interrupt might be lowered by the hardware. In the result, if the interrupt is short enough, the parent interrupt is still pending while the GPIO interrupt is cleared; chained_irq_enter() never gets called and the system hangs trying to service the parent interrupt. Moving chained_irq_enter() and chained_irq_exit() outside the for loop ensures that they are called even when GPIO interrupt is lowered by the hardware. The similar code with chained_irq_enter() / chained_irq_exit() functions wrapping interrupt checking loop may be found in many other drivers: ``` grep -r -A 10 chained_irq_enter drivers/pinctrl ```	5.5	More Details
CVE-2024-50197	In the Linux kernel, the following vulnerability has been resolved: pinctrl: intel: platform: fix error path in device_for_each_child_node() The device_for_each_child_node() loop requires calls to fwnode_handle_put() upon early returns to decrement the refcount of the child node and avoid leaking memory if that error path is triggered. There is one early returns within that loop in intel_platform_pinctrl_prepare_community(), but fwnode_handle_put() is missing. Instead of adding the missing call, the scoped version of the loop can be used to simplify the code and avoid mistakes in the future if new early returns are added, as the child node is only used for parsing, and it is never assigned.	5.5	More Details
CVE-2024-50198	In the Linux kernel, the following vulnerability has been resolved: iio: light: veml6030: fix IIO device retrieval from embedded device The dev pointer that is received as an argument in the in_illuminance_period_available_show function references the device embedded in the IIO device, not in the i2c client. dev_to_iio_dev() must be used to accessthe right data. The current implementation leads to a segmentation fault on every attempt to read the attribute because indio_dev gets a NULL assignment. This bug has been present since the first appearance of the driver, apparently since the last version (V6) before getting applied. A constant attribute was used until then, and the last modifications might have not been tested again.	5.5	More Details
CVE-2024-50201	In the Linux kernel, the following vulnerability has been resolved: drm/radeon: Fix encoder->possible_clones Include the encoder itself in its possible_clones bitmask. In the past nothing validated that drivers were populating possible_clones correctly, but that changed in commit 74d2aacbe840 ("drm: Validate encoder->possible_clones"). Looks like radeon never got the memo and is still not following the rules 100% correctly. This results in some warnings during driver initialization: Bogus possible_clones: [ENCODER:46:TV-46] possible_clones=0x4 (full encoder mask=0x7) WARNING: CPU: 0 PID: 170 at drivers/gpu/drm/drm_mode_config.c:615 drm_mode_config_validate+0x113/0x39c ... (cherry picked from commit 3b6e7d40649c0d75572039aff9d0911864c689db)	5.5	More Details
CVE-2024-50202	In the Linux kernel, the following vulnerability has been resolved: nilfs2: propagate directory read errors from nilfs_find_entry() Syzbot reported that a task hang occurs in vcs_open() during a fuzzing test for nilfs2. The root cause of this problem is that in nilfs_find_entry(), which searches for directory entries, ignores errors when loading a directory page/folio via nilfs_get_folio() fails. If the filesystem images is corrupted, and the i_size of the directory inode is large, and the directory page/folio is successfully read but fails the sanity check, for example when it is zero-filled, nilfs_check_folio() may continue to spit out error messages in bursts. Fix this issue by propagating the error to the callers when loading a page/folio fails in nilfs_find_entry(). The current interface of nilfs_find_entry() and its callers is outdated and cannot propagate error codes such as -EIO and -ENOMEM returned via nilfs_find_entry(), so fix it together.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50204	In the Linux kernel, the following vulnerability has been resolved: fs: don't try and remove empty rbtree node When copying a namespace we won't have added the new copy into the namespace rbtree until after the copy succeeded. Calling free_mnt_ns() will try to remove the copy from the rbtree which is invalid. Simply free the namespace skeleton directly.	5.5	More Details
CVE-2024-50207	In the Linux kernel, the following vulnerability has been resolved: ring-buffer: Fix reader locking when changing the sub buffer order The function ring_buffer_subbuf_order_set() updates each ring_buffer_per_cpu and installs new sub buffers that match the requested page order. This operation may be invoked concurrently with readers that rely on some of the modified data, such as the head bit (RB_PAGE_HEAD), or the ring_buffer_per_cpu.pages and reader_page pointers. However, no exclusive access is acquired by ring_buffer_subbuf_order_set(). Modifying the mentioned data while a reader also operates on them can then result in incorrect memory access and various crashes. Fix the problem by taking the reader_lock when updating a specific ring_buffer_per_cpu in ring_buffer_subbuf_order_set().	5.5	More Details
CVE-2024-50172	In the Linux kernel, the following vulnerability has been resolved: RDMA/bnxt_re: Fix a possible memory leak In bnxt_re_setup_chip_ctx() when bnxt_qplib_map_db_bar() fails driver is not freeing the memory allocated for "rdev->chip_ctx".	5.5	More Details
CVE-2024-35427	vmir e8117 was discovered to contain a segmentation violation via the export_function function at /src/vmir_wasm_parser.c.	5.5	More Details
CVE-2024-50208	In the Linux kernel, the following vulnerability has been resolved: RDMA/bnxt_re: Fix a bug while setting up Level-2 PBL pages Avoid memory corruption while setting up Level-2 PBL pages for the non MR resources when num_pages > 256K. There will be a single PDE page address (contiguous pages in the case of > PAGE_SIZE), but, current logic assumes multiple pages, leading to invalid memory access after 256K PBL entries in the PDE.	5.5	More Details
CVE-2024-35424	vmir e8117 was discovered to contain a segmentation violation via the import_function function at /src/vmir_wasm_parser.c.	5.5	More Details
CVE-2024-21949	Improper validation of user input in the NPU driver could allow an attacker to provide a buffer with unexpected size, potentially leading to system crash.	5.5	More Details
CVE-2024-35421	vmir e8117 was discovered to contain a segmentation violation via the wasm_parse_block function at /src/vmir_wasm_parser.c.	5.5	More Details
CVE-2024-50210	In the Linux kernel, the following vulnerability has been resolved: posix-clock: posix-clock: Fix unbalanced locking in pc_clock_settime() If get_clock_desc() succeeds, it calls fget() for the clockid's fd, and get the clk->rwsem read lock, so the error path should release the lock to make the lock balance and fput the clockid's fd to make the refcount balance and release the fd related resource. However the below commit left the error path locked behind resulting in unbalanced locking. Check timespec64_valid_strict() before get_clock_desc() to fix it, because the "ts" is not changed after that. [pabeni@redhat.com: fixed commit message typo]	5.5	More Details
CVE-2024-35419	wac commit 385e1 was discovered to contain a heap overflow via the load_module function at /wac-asan/wa.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted wasm file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50194	In the Linux kernel, the following vulnerability has been resolved: arm64: probes: Fix uprobes for big-endian kernels The arm64 uprobes code is broken for big-endian kernels as it doesn't convert the in-memory instruction encoding (which is always little-endian) into the kernel's native endianness before analyzing and simulating instructions. This may result in a few distinct problems: * The kernel may may erroneously reject probing an instruction which can safely be probed. * The kernel may erroneously erroneously permit stepping an instruction out-of-line when that instruction cannot be stepped out-of-line safely. * The kernel may erroneously simulate instruction incorrectly dur to interpretting the byte-swapped encoding. The endianness mismatch isn't caught by the compiler or sparse because: * The arch_uprobe::{insn,ixol} fields are encoded as arrays of u8, so the compiler and sparse have no idea these contain a little-endian 32-bit value. The core uprobes code populates these with a memcpy() which similarly does not handle endianness. * While the uprobe_opcode_t type is an alias for __le32, both arch_uprobe_analyze_insn() and arch_uprobe_skip_sstep() cast from u8[] to the similarly-named probe_opcode_t, which is an alias for u32. Hence there is no endianness conversion warning. Fix this by changing the arch_uprobe::{insn,ixol} fields to __le32 and adding the appropriate __le32_to_cpu() conversions prior to consuming the instruction encoding. The core uprobes copies these fields as opaque ranges of bytes, and so is unaffected by this change. At the same time, remove MAX_UINSN_BYTES and consistently use AARCH64_INSN_SIZE for clarity. Tested with the following:	#include <stdio.h>	#include <stdbool.h>		#define noinline __attribute__((noinline))		static noinline void *adrp_self(void)	{	void *addr;		asm volatile(	" adrp %x0, adrp_self\n"	" add %x0, %x0, :lo12:adrp_self\n"	: "=r" (addr));	}			int main(int argc, char *argv)	{	void *ptr = adrp_self();	bool equal = (ptr == adrp_self);		printf("adrp_self => %p\n"	"adrp_self() => %p\n"	"%s\n",	adrp_self, ptr, equal ? "EQUAL" : "NOT EQUAL");		return 0;	} .... where the adrp_self() function was compiled to:	00000000004007e0 <adrp_self>:	4007e0: 90000000 adrp x0, 400000 <__ehdr_start>	4007e4: 911f8000 add x0, x0, #0x7e0	4007e8: d65f03c0 ret Before this patch, the ADRP is not recognized, and is assumed to be steppable, resulting in corruption of the result:	# ./adrp-self	adrp_self => 0x4007e0	adrp_self() => 0x4007e0	EQUAL	# echo 'p /root/adrp-self:0x007e0' > /sys/kernel/tracing/uprobe_events	# echo 1 > /sys/kernel/tracing/events/uprobes/enable	# ./adrp-self	adrp_self => 0x4007e0	adrp_self() => 0xfffffffff7e0	NOT EQUAL After this patch, the ADRP is correctly recognized and simulated:	# ./adrp-self	adrp_self => 0x4007e0	adrp_self() => 0x4007e0	EQUAL	#	# echo 'p /root/adrp-self:0x007e0' > /sys/kernel/tracing/uprobe_events	# echo 1 > /sys/kernel/tracing/events/uprobes/enable	# ./adrp-self	adrp_self => 0x4007e0	adrp_self() => 0x4007e0	EQUAL	5.5	More Details
CVE-2024-9775	The Anih - Creative Agency WordPress Theme theme for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2024 due to an incomplete blacklist, insufficient input sanitization, and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	5.5	More Details
CVE-2024-50191	In the Linux kernel, the following vulnerability has been resolved: ext4: don't set SB_RDONLY after filesystem errors When the filesystem is mounted with errors=remount-ro, we were setting SB_RDONLY flag to stop all filesystem modifications. We knew this misses proper locking (sb->s_umount) and does not go through proper filesystem remount procedure but it has been the way this worked since early ext2 days and it was good enough for catastrophic situation damage mitigation. Recently, syzbot has found a way (see link) to trigger warnings in filesystem freezing because the code got confused by SB_RDONLY changing under its hands. Since these days we set EXT4_FLAGS_SHUTDOWN on the superblock which is enough to stop all filesystem modifications, modifying SB_RDONLY shouldn't be needed. So stop doing that.	5.5	More Details
CVE-2024-47535	Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. An unsafe reading of environment file could potentially cause a denial of service in Netty. When loaded on an Windows application, Netty attempts to load a file that does not exist. If an attacker creates such a large file, the Netty application crashes. This vulnerability is fixed in 4.1.115.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50213	In the Linux kernel, the following vulnerability has been resolved: drm/tests: hdmi: Fix memory leaks in drm_display_mode_from_cea_vic() modprobe drm_hdmi_state_helper_test and then rmmod it, the following memory leak occurs. The `mode` allocated in drm_mode_duplicate() called by drm_display_mode_from_cea_vic() is not freed, which cause the memory leak: unreferenced object 0xffffff80ccd18100 (size 128): comm "kunit_try_catch", pid 1851, jiffies 4295059695 hex dump (first 32 bytes): 57 62 00 00 80 02 90 02 f0 02 20 03 00 00 e0 01 Wb..... ..... ea 01 ec 01 0d 02 00 00 0a 00 00 00 00 00 00 00 ..... backtrace (crc c2f1aa95): [<000000000f10b11b>] kmemleak_alloc+0x34/0x40 [<000000001cd4cf73>] __kmalloc_cache_noprof+0x26c/0x2f4 [<00000000f1f3cffa>] drm_mode_duplicate+0x44/0x19c [<000000008cbeef13>] drm_display_mode_from_cea_vic+0x88/0x98 [<0000000019daaacf>] 0xffffffedc11ae69c [<000000000aad0f85>] kunit_try_run_case+0x13c/0x3ac [<00000000a9210bac>] kunit_generic_run_threadfn_adapter+0x80/0xec [<000000000a0b2e9e>] kthread+0x2e8/0x374 [<00000000bd668858>] ret_from_fork+0x10/0x20 ..... Free `mode` by using drm_kunit_display_mode_from_cea_vic() to fix it.	5.5	More Details
CVE-2024-50173	In the Linux kernel, the following vulnerability has been resolved: drm/panthor: Fix access to uninitialized variable in tick_ctx_cleanup() The group variable can't be used to retrieve ptdev in our second loop, because it points to the previously iterated list_head, not a valid group. Get the ptdev object from the scheduler instead.	5.5	More Details
CVE-2024-50175	In the Linux kernel, the following vulnerability has been resolved: media: qcom: camss: Remove use_count guard in stop_streaming The use_count check was introduced so that multiple concurrent Raw Data Interfaces RDIs could be driven by different virtual channels VCs on the CSIPHY input driving the video pipeline. This is an invalid use of use_count though as use_count pertains to the number of times a video entity has been opened by user-space not the number of active streams. If use_count and stream-on count don't agree then stop_streaming() will break as is currently the case and has become apparent when using CAMSS with libcamera's released softisp 0.3. The use of use_count like this is a bit hacky and right now breaks regular usage of CAMSS for a single stream case. Stopping qcam results in the splat below, and then it cannot be started again and any attempts to do so fails with -EBUSY. [1265.509831] WARNING: CPU: 5 PID: 919 at drivers/media/common/videobuf2/videobuf2-core.c:2183 __vb2_queue_cancel+0x230/0x2c8 [videobuf2_common] ... [1265.510630] Call trace: [1265.510636] __vb2_queue_cancel+0x230/0x2c8 [videobuf2_common] [1265.510648] vb2_core_streamoff+0x24/0xcc [videobuf2_common] [1265.510660] vb2_ioctl_streamoff+0x5c/0xa8 [videobuf2_v4l2] [1265.510673] v4l_streamoff+0x24/0x30 [videodev] [1265.510707] __video_do_ioctl+0x190/0x3f4 [videodev] [1265.510732] video_usercopy+0x304/0x8c4 [videodev] [1265.510757] video_ioctl2+0x18/0x34 [videodev] [1265.510782] v4l2_ioctl+0x40/0x60 [videodev] ... [1265.510944] videobuf2_common: driver bug: stop_streaming operation is leaving buffer 0 in active state [1265.511175] videobuf2_common: driver bug: stop_streaming operation is leaving buffer 1 in active state [1265.511398] videobuf2_common: driver bug: stop_streaming operation is leaving buffer 2 in active st One CAMSS specific way to handle multiple VCs on the same RDI might be: - Reference count each pipeline enable for CSIPHY, CSID, VFE and RDIx. - The video buffers are already associated with msm_vfeN_rdiX so release video buffers when told to do so by stop_streaming. - Only release the power-domains for the CSIPHY, CSID and VFE when their internal refcounts drop. Either way refusing to release video buffers based on use_count is erroneous and should be reverted. The silicon enabling code for selecting VCs is perfectly fine. Its a "known missing feature" that concurrent VCs won't work with CAMSS right now. Initial testing with this code didn't show an error but, SoftISP and "real" usage with Google Hangouts breaks the upstream code pretty quickly, we need to do a partial revert and take another pass at VCs. This commit partially reverts commit 89013969e232 ("media: camss: sm8250: Pipeline starting and stopping for multiple virtual channels")	5.5	More Details
CVE-2024-50176	In the Linux kernel, the following vulnerability has been resolved: remoteproc: k3-r5: Fix error handling when power-up failed By simply bailing out, the driver was violating its rule and internal assumptions that either both or no rproc should be initialized. E.g., this could cause the first core to be available but not the second one, leading to crashes on its shutdown later on while trying to dereference that second instance.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50177	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: fix a UBSAN warning in DML2.1 When programming phantom pipe, since cursor_width is explicity set to 0, this causes calculation logic to trigger overflow for an unsigned int triggering the kernel's UBSAN check as below: [40.962845] UBSAN: shift-out-of-bounds in /tmp/amd.EfpumTkO/amd/amdgpu/../display/dc/dml2/dml21/src/dml2_core/dml2_core_dcn4_calcs.c:3312:34 [40.962849] shift exponent 4294967170 is too large for 32-bit type 'unsigned int' [40.962852] CPU: 1 PID: 1670 Comm: gnome-shell Tainted: G W OE 6.5.0-41-generic #41~22.04.2-Ubuntu [40.962854] Hardware name: Gigabyte Technology Co., Ltd. X670E AORUS PRO X/X670E AORUS PRO X, BIOS F21 01/10/2024 [40.962856] Call Trace: [40.962857] <TASK> [40.962860] dump_stack_lvl+0x48/0x70 [40.962870] dump_stack+0x10/0x20 [40.962872] __ubsan_handle_shift_out_of_bounds+0x1ac/0x360 [40.962878] calculate_cursor_req_attributes.cold+0x1b/0x28 [amdgpu] [40.963099] dml_core_mode_support+0x6b91/0x16bc0 [amdgpu] [40.963327] ? srso_alias_return_thunk+0x5/0x7f [40.963331] ? CalculateWatermarksMALLUseAndDRAMSpeedChangeSupport+0x18b8/0x2790 [amdgpu] [40.963534] ? srso_alias_return_thunk+0x5/0x7f [40.963536] ? dml_core_mode_support+0xb3db/0x16bc0 [amdgpu] [40.963730] dml2_core_calcs_mode_support_ex+0x2c/0x90 [amdgpu] [40.963906] ? srso_alias_return_thunk+0x5/0x7f [40.963909] ? dml2_core_calcs_mode_support_ex+0x2c/0x90 [amdgpu] [40.964078] core_dcn4_mode_support+0x72/0xbf0 [amdgpu] [40.964247] dml2_top_optimization_perform_optimization_phase+0x1d3/0x2a0 [amdgpu] [40.964420] dml2_build_mode_programming+0x23d/0x750 [amdgpu] [40.964587] dml21_validate+0x274/0x770 [amdgpu] [40.964761] ? srso_alias_return_thunk+0x5/0x7f [40.964763] ? resource_append_dpp_pipes_for_plane_composition+0x27c/0x3b0 [amdgpu] [40.964942] dml2_validate+0x504/0x750 [amdgpu] [40.965117] ? dml21_copy+0x95/0xb0 [amdgpu] [40.965291] ? srso_alias_return_thunk+0x5/0x7f [40.965295] dcn401_validate_bandwidth+0x4e/0x70 [amdgpu] [40.965491] update_planes_and_stream_state+0x38d/0x5c0 [amdgpu] [40.965672] update_planes_and_stream_v3+0x52/0x1e0 [amdgpu] [40.965845] ? srso_alias_return_thunk+0x5/0x7f [40.965849] dc_update_planes_and_stream+0x71/0xb0 [amdgpu] Fix this by adding a guard for checking cursor width before triggering the size calculation.	5.5	More Details
CVE-2024-50178	In the Linux kernel, the following vulnerability has been resolved: cpufreq: loongson3: Use raw_smp_processor_id() in do_service_request() Use raw_smp_processor_id() instead of plain smp_processor_id() in do_service_request(), otherwise we may get some errors with the driver enabled: BUG: using smp_processor_id() in preemptible [00000000] code: (udev-worker)/208 caller is loongson3_cpufreq_probe+0x5c/0x250 [loongson3_cpufreq]	5.5	More Details
CVE-2024-50179	In the Linux kernel, the following vulnerability has been resolved: ceph: remove the incorrect Fw reference check when dirtying pages When doing the direct-io reads it will also try to mark pages dirty, but for the read path it won't hold the Fw caps and there is case will it get the Fw reference.	5.5	More Details
CVE-2024-50181	In the Linux kernel, the following vulnerability has been resolved: clk: imx: Remove CLK_SET_PARENT_GATE for DRAM mux for i.MX7D For i.MX7D DRAM related mux clock, the clock source change should ONLY be done done in low level asm code without accessing DRAM, and then calling clk API to sync the HW clock status with clk tree, it should never touch real clock source switch via clk API, so CLK_SET_PARENT_GATE flag should NOT be added, otherwise, DRAM's clock parent will be disabled when DRAM is active, and system will hang.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50182	In the Linux kernel, the following vulnerability has been resolved: secretmem: disable memfd_secret() if arch cannot set direct map Return -ENOSYS from memfd_secret() syscall if !can_set_direct_map(). This is the case for example on some arm64 configurations, where marking 4k PTEs in the direct map not present can only be done if the direct map is set up at 4k granularity in the first place (as ARM's break-before-make semantics do not easily allow breaking apart large/gigantic pages). More precisely, on arm64 systems with !can_set_direct_map(), set_direct_map_invalid_noflush() is a no-op, however it returns success (0) instead of an error. This means that memfd_secret will seemingly "work" (e.g. syscall succeeds, you can mmap the fd and fault in pages), but it does not actually achieve its goal of removing its memory from the direct map. Note that with this patch, memfd_secret() will start erroring on systems where can_set_direct_map() returns false (arm64 with CONFIG_RODATA_FULL_DEFAULT_ENABLED=n, CONFIG_DEBUG_PAGEALLOC=n and CONFIG_KFENCE=n), but that still seems better than the current silent failure. Since CONFIG_RODATA_FULL_DEFAULT_ENABLED defaults to 'y', most arm64 systems actually have a working memfd_secret() and aren't be affected. From going through the iterations of the original memfd_secret patch series, it seems that disabling the syscall in these scenarios was the intended behavior [1] (preferred over having set_direct_map_invalid_noflush return an error as that would result in SIGBUSes at page-fault time), however the check for it got dropped between v16 [2] and v17 [3], when secretmem moved away from CMA allocations. [1]: https://lore.kernel.org/lkml/20201124164930.GK8537@kernel.org/ [2]: https://lore.kernel.org/lkml/20210121122723.3446-11-rppt@kernel.org/#t [3]: https://lore.kernel.org/lkml/20201125092208.12544-10-rppt@kernel.org/	5.5	More Details
CVE-2024-50184	In the Linux kernel, the following vulnerability has been resolved: virtio_pmem: Check device status before requesting flush If a pmem device is in a bad status, the driver side could wait for host ack forever in virtio_pmem_flush(), causing the system to hang. So add a status check in the beginning of virtio_pmem_flush() to return early if the device is not activated.	5.5	More Details
CVE-2024-50185	In the Linux kernel, the following vulnerability has been resolved: mptcp: handle consistently DSS corruption Bugged peer implementation can send corrupted DSS options, consistently hitting a few warning in the data path. Use DEBUG_NET assertions, to avoid the splat on some builds and handle consistently the error, dumping related MIBs and performing fallback and/or reset according to the subflow type.	5.5	More Details
CVE-2024-50187	In the Linux kernel, the following vulnerability has been resolved: drm/vc4: Stop the active perfmon before being destroyed Upon closing the file descriptor, the active performance monitor is not stopped. Although all perfmons are destroyed in `vc4_perfmon_close_file()`, the active performance monitor's pointer (`vc4->active_perfmon`) is still retained. If we open a new file descriptor and submit a few jobs with performance monitors, the driver will attempt to stop the active performance monitor using the stale pointer in `vc4->active_perfmon`. However, this pointer is no longer valid because the previous process has already terminated, and all performance monitors associated with it have been destroyed and freed. To fix this, when the active performance monitor belongs to a given process, explicitly stop it before destroying and freeing it.	5.5	More Details
CVE-2024-50188	In the Linux kernel, the following vulnerability has been resolved: net: phy: dp83869: fix memory corruption when enabling fiber When configuring the fiber port, the DP83869 PHY driver incorrectly calls linkmode_set_bit() with a bit mask (1 << 10) rather than a bit number (10). This corrupts some other memory location -- in case of arm64 the priv pointer in the same structure. Since the advertising flags are updated from supported at the end of the function the incorrect line isn't needed at all and can be removed.	5.5	More Details
CVE-2024-50189	In the Linux kernel, the following vulnerability has been resolved: HID: amd_sfh: Switch to device-managed dmam_alloc_coherent() Using the device-managed version allows to simplify clean-up in probe() error path. Additionally, this device-managed ensures proper cleanup, which helps to resolve memory errors, page faults, btrfs going read-only, and btrfs disk corruption.	5.5	More Details
CVE-2024-50190	In the Linux kernel, the following vulnerability has been resolved: ice: fix memleak in ice_init_tx_topology() Fix leak of the FW blob (DDP pkg). Make ice_cfg_tx_topo() const-correct, so ice_init_tx_topology() can avoid copying whole FW blob. Copy just the topology section, and only when needed. Reuse the buffer allocated for the read of the current topology. This was found by kmemleak, with the following trace for each PF: [<ffffffff8761044d>] kmemdup_noprof+0x1d/0x50 [<ffffffffc0a0a480>] ice_init_ddp_config+0x100/0x220 [ice] [<ffffffffc0a0da7f>] ice_init_dev+0x6f/0x200 [ice] [<ffffffffc0a0dc49>] ice_init+0x29/0x560 [ice] [<ffffffffc0a10c1d>] ice_probe+0x21d/0x310 [ice] Constify ice_cfg_tx_topo() @buf parameter. This cascades further down to few more functions.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49527	Animate versions 23.0.7, 24.0.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-50245	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: Fix possible deadlock in mi_read Mutex lock with another subclass used in ni_lock_dir().	5.5	More Details
CVE-2024-50248	In the Linux kernel, the following vulnerability has been resolved: ntfs3: Add bounds checking to mi_enum_attr() Added bounds checking to make sure that every attr don't stray beyond valid memory region.	5.5	More Details
CVE-2024-49510	InDesign Desktop versions ID18.5.3, ID19.5 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-47436	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-47454	Illustrator versions 28.7.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-47455	Illustrator versions 28.7.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-47456	Illustrator versions 28.7.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-47457	Illustrator versions 28.7.1 and earlier are affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-46955	An issue was discovered in psi/zcolor.c in Artifex Ghostscript before 10.04.0. There is an out-of-bounds read when reading color in Indexed color space.	5.5	More Details
CVE-2024-47458	Bridge versions 13.0.9, 14.1.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-20532	A vulnerability in the API of Cisco ISE could allow an authenticated, remote attacker to read and delete arbitrary files on an affected device. To exploit this vulnerability, the attacker would need valid Super Admin credentials. This vulnerability is due to insufficient validation of user-supplied parameters in API requests. An attacker could exploit this vulnerability by sending a crafted API request to an affected device. A successful exploit could allow the attacker to read or delete arbitrary files on the underlying operating system.	5.5	More Details
CVE-2024-20531	A vulnerability in the API of Cisco ISE could allow an authenticated, remote attacker to read arbitrary files on the underlying operating system of an affected device and conduct a server-side request forgery (SSRF) attack through an affected device. To exploit this vulnerability, the attacker would need valid Super Admin credentials. This vulnerability is due to improper handling of XML External Entity (XXE) entries when parsing XML input. An attacker could exploit this vulnerability by sending a crafted API request to an affected device. A successful exploit could allow the attacker to read arbitrary files on the underlying operating system or conduct an SSRF attack through the affected device.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51490	Ampache is a web based audio/video streaming application and file manager. This vulnerability exists in the interface section of the Ampache menu, where users can change "Custom URL - Logo". This section is not properly sanitized, allowing for the input of strings that can execute JavaScript. This issue has been addressed in version 7.0.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	5.5	More Details
CVE-2024-49404	Improper Access Control in Samsung Video Player prior to versions 7.3.29.1 in Android 12, 7.3.36.1 in Android 13, and 7.3.41.230 in Android 14 allows physical attackers to access video file of other users.	5.5	More Details
CVE-2024-50263	In the Linux kernel, the following vulnerability has been resolved: fork: only invoke khugepaged, ksm hooks if no error There is no reason to invoke these hooks early against an mm that is in an incomplete state. The change in commit d24062914837 ("fork: use __mt_dup() to duplicate maple tree in dup_mmap()") makes this more pertinent as we may be in a state where entries in the maple tree are not yet consistent. Their placement early in dup_mmap() only appears to have been meaningful for early error checking, and since functionally it'd require a very small allocation to fail (in practice 'too small to fail') that'd only occur in the most dire circumstances, meaning the fork would fail or be OOM'd in any case. Since both khugepaged and KSM tracking are there to provide optimisations to memory performance rather than critical functionality, it doesn't really matter all that much if, under such dire memory pressure, we fail to register an mm with these. As a result, we follow the example of commit d2081b2bf819 ("mm: khugepaged: make khugepaged_enter() void function") and make ksm_fork() a void function also. We only expose the mm to these functions once we are done with them and only if no error occurred in the fork operation.	5.5	More Details
CVE-2024-50145	In the Linux kernel, the following vulnerability has been resolved: octeon_ep: Add SKB allocation failures handling in __octep_oq_process_rx() build_skb() returns NULL in case of a memory allocation failure so handle it inside __octep_oq_process_rx() to avoid NULL pointer dereference. __octep_oq_process_rx() is called during NAPI polling by the driver. If skb allocation fails, keep on pulling packets out of the Rx DMA queue: we shouldn't break the polling immediately and thus falsely indicate to the octep_napi_poll() that the Rx pressure is going down. As there is no associated skb in this case, don't process the packets and don't push them up the network stack - they are skipped. Helper function is implemented to unmmap/flush all the fragment buffers used by the dropped packet. 'alloc_failures' counter is incremented to mark the skb allocation error in driver statistics. Found by Linux Verification Center (linuxtesting.org) with SVACE.	5.5	More Details
CVE-2020-10367	Certain Cypress (and Broadcom) Wireless Combo chips, when a January 2021 firmware update is not present, allow memory access via a "Spectra" attack.	5.5	More Details
CVE-2024-51486	Ampache is a web based audio/video streaming application and file manager. The vulnerability exists in the interface section of the Ampache menu, where users can change the "Custom URL-Favicon". This section is not properly sanitized, allowing for the input of strings that can execute JavaScript. This issue has been addressed in version 7.0.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	5.5	More Details
CVE-2024-20529	A vulnerability in the API of Cisco ISE could allow an authenticated, remote attacker to read and delete arbitrary files on an affected device. To exploit this vulnerability, the attacker would need valid Super Admin credentials. This vulnerability is due to insufficient validation of user-supplied parameters in API requests. An attacker could exploit this vulnerability by sending a crafted API request to an affected device. A successful exploit could allow the attacker to read or delete arbitrary files on the underlying operating system.	5.5	More Details
CVE-2020-10369	Certain Cypress (and Broadcom) Wireless Combo chips, when a January 2021 firmware update is not present, allow inferences about memory content via a "Spectra" attack.	5.5	More Details
CVE-2024-20527	A vulnerability in the API of Cisco ISE could allow an authenticated, remote attacker to read and delete arbitrary files on an affected device. To exploit this vulnerability, the attacker would need valid Super Admin credentials. This vulnerability is due to insufficient validation of user-supplied parameters in API requests. An attacker could exploit this vulnerability by sending a crafted API request to an affected device. A successful exploit could allow the attacker to read or delete arbitrary files on the underlying operating system.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47440	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-47439	Substance3D - Painter versions 10.1.0 and earlier are affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-47438	Substance3D - Painter versions 10.1.0 and earlier are affected by a Write-what-where Condition vulnerability that could lead to a memory leak. This vulnerability allows an attacker to write a controlled value at a controlled memory location, which could result in the disclosure of sensitive memory content. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-47437	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-49511	InDesign Desktop versions ID18.5.3, ID19.5 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-47453	Illustrator versions 28.7.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-47449	Audition versions 23.6.9, 24.4.6 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-50255	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci: fix null-ptr-deref in hci_read_supported_codecs Fix __hci_cmd_sync_sk() to return not NULL for unknown opcodes. __hci_cmd_sync_sk() returns NULL if a command returns a status event. However, it also returns NULL where an opcode doesn't exist in the hci_cc table because hci_cmd_complete_evt() assumes status = skb->data[0] for unknown opcodes. This leads to null-ptr-deref in cmd_sync for HCI_OP_READ_LOCAL_CODECS as there is no hci_cc for HCI_OP_READ_LOCAL_CODECS, which always assumes status = skb->data[0]. KASAN: null-ptr-deref in range [0x0000000000000070-0x0000000000000077] CPU: 1 PID: 2000 Comm: kworker/u9:5 Not tainted 6.9.0-ga6bcb805883c-dirty #10 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 Workqueue: hci7 hci_power_on RIP: 0010:hci_read_supported_codecs+0xb9/0x870 net/bluetooth/hci_codec.c:138 Code: 08 48 89 ef e8 b8 c1 8f fd 48 8b 75 00 e9 96 00 00 00 49 89 c6 48 ba 00 00 00 00 00 fc ff df 4c 8d 60 70 4c 89 e3 48 c1 eb 03 <0f> b6 04 13 84 c0 0f 85 82 06 00 00 41 83 3c 24 02 77 0a e8 bf 78 RSP: 0018:ffff888120bafac8 EFLAGS: 00010212 RAX: 0000000000000000 RBX: 000000000000000e RCX: ffff8881173f0040 RDX: dfffc0000000000 RSI: ffffffffa58496c0 RDI: ffff88810b9ad1e4 RBP: ffff88810b9ac000 R08: ffffffffa77882a7 R09: 1ffffffff4ef1054 R10: dfffc0000000000 R11: fffffbfff4ef1055 R12: 0000000000000070 R13: 0000000000000000 R14: 0000000000000000 R15: ffff88810b9ac000 FS: 0000000000000000(0000) GS:ffff8881f6c00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f6ddaa3439e CR3: 0000000139764003 CR4: 0000000000770ef0 PKRU: 55555554 Call Trace: <TASK> hci_read_local_codecs_sync net/bluetooth/hci_sync.c:4546 [inline] hci_init_stage_sync net/bluetooth/hci_sync.c:3441 [inline] hci_init4_sync net/bluetooth/hci_sync.c:4706 [inline] hci_init_sync net/bluetooth/hci_sync.c:4742 [inline] hci_dev_init_sync net/bluetooth/hci_sync.c:4912 [inline] hci_dev_open_sync+0x19a9/0x2d30 net/bluetooth/hci_sync.c:4994 hci_dev_do_open net/bluetooth/hci_core.c:483 [inline] hci_power_on+0x11e/0x560 net/bluetooth/hci_core.c:1015 process_one_work kernel/workqueue.c:3267 [inline] process_scheduled_works+0x8ef/0x14f0 kernel/workqueue.c:3348 worker_thread+0x91f/0xe50 kernel/workqueue.c:3429 kthread+0x2cb/0x360 kernel/kthread.c:388 ret_from_fork+0x4d/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-2024-50144	In the Linux kernel, the following vulnerability has been resolved: drm/xe: fix unbalanced rpm put() with fence_fini() Currently we can call fence_fini() twice if something goes wrong when sending the GuC CT for the tlb request, since we signal the fence and return an error, leading to the caller also calling fini() on the error path in the case of stack version of the flow, which leads to an extra rpm put() which might later cause device to enter suspend when it shouldn't. It looks like we can just drop the fini() call since the fence signaller side will already call this for us. There are known mysterious splats with device going to sleep even with an rpm ref, and this could be one candidate. v2 (Matt B): - Prefer warning if we detect double fini() (cherry picked from commit cfcbc0520d5055825f0647ab922b655688605183)	5.5	More Details
CVE-2024-50249	In the Linux kernel, the following vulnerability has been resolved: ACPI: CPPC: Make rmw_lock a raw_spin_lock The following BUG was triggered: ============================== [BUG: Invalid wait context] 6.12.0-rc2-XXX #406 Not tainted ----------------------------- kworker/1:1/62 is trying to lock: ffffff8801593030 (&cpc_ptr->rmw_lock){+.+.}-{3:3}, at: cpc_write+0xcc/0x370 other info that might help us debug this: context-{5:5} 2 locks held by kworker/1:1/62: #0: ffffff897ef5ec98 (&rq->__lock){-.-.}-{2:2}, at: raw_spin_rq_lock_nested+0x2c/0x50 #1: ffffff880154e238 (&sg_policy->update_lock){....}-{2:2}, at: sugov_update_shared+0x3c/0x280 stack backtrace: CPU: 1 UID: 0 PID: 62 Comm: kworker/1:1 Not tainted 6.12.0-rc2-g9654bd3e8806 #406 Workqueue: 0x0 (events) Call trace: dump_backtrace+0xa4/0x130 show_stack+0x20/0x38 dump_stack_lvl+0x90/0xd0 dump_stack+0x18/0x28 __lock_acquire+0x480/0x1ad8 lock_acquire+0x114/0x310 _raw_spin_lock+0x50/0x70 cpc_write+0xcc/0x370 cppc_set_perf+0xa0/0x3a8 cppc_cpufreq_fast_switch+0x40/0xc0 cpufreq_driver_fast_switch+0x4c/0x218 sugov_update_shared+0x234/0x280 update_load_avg+0x6ec/0x7b8 dequeue_entities+0x108/0x830 dequeue_task_fair+0x58/0x408 __schedule+0x4f0/0x1070 schedule+0x54/0x130 worker_thread+0xc0/0x2e8 kthread+0x130/0x148 ret_from_fork+0x10/0x20 sugov_update_shared() locks a raw_spinlock while cpc_write() locks a spinlock. To have a correct wait-type order, update rmw_lock to a raw spinlock and ensure that interrupts will be disabled on the CPU holding it. [rjw: Changelog edits]	5.5	More Details
CVE-2024-50142	In the Linux kernel, the following vulnerability has been resolved: xfrm: validate new SA's prefixlen using SA family when sel.family is unset This expands the validation introduced in commit 07bf7908950a ("xfrm: Validate address prefix lengths in the xfrm selector.") syzbot created an SA with usersa.sel.family = AF_UNSPEC usersa.sel.prefixlen_s = 128 usersa.family = AF_INET Because of the AF_UNSPEC selector, verify_newsa_info doesn't put limits on prefixlen_{s,d}. But then copy_from_user_state sets x->sel.family to usersa.family (AF_INET). Do the same conversion in verify_newsa_info before validating prefixlen_{s,d}, since that's how prefixlen is going to be used later on.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50252	In the Linux kernel, the following vulnerability has been resolved: mlxsw: spectrum_ipip: Fix memory leak when changing remote IPv6 address The device stores IPv6 addresses that are used for encapsulation in linear memory that is managed by the driver. Changing the remote address of an ip6gre net device never worked properly, but since cited commit the following reproducer [1] would result in a warning [2] and a memory leak [3]. The problem is that the new remote address is never added by the driver to its hash table (and therefore the device) and the old address is never removed from it. Fix by programming the new address when the configuration of the ip6gre net device changes and removing the old one. If the address did not change, then the above would result in increasing the reference count of the address and then decreasing it. [1] # ip link add name bla up type ip6gre local 2001:db8:1::1 remote 2001:db8:2::1 tos inherit ttl inherit # ip link set dev bla type ip6gre remote 2001:db8:3::1 # ip link del dev bla # devlink dev reload pci/0000:01:00.0 [2] WARNING: CPU: 0 PID: 1682 at drivers/net/ethernet/mellanox/mlxsw/spectrum.c:3002 mlxsw_sp_ipv6_addr_put+0x140/0x1d0 Modules linked in: CPU: 0 UID: 0 PID: 1682 Comm: ip Not tainted 6.12.0-rc3-custom-g86b5b55bc835 #151 Hardware name: Nvidia SN5600/VMOD0013, BIOS 5.13 05/31/2023 RIP: 0010:mlxsw_sp_ipv6_addr_put+0x140/0x1d0 [...] Call Trace: <TASK> mlxsw_sp_router_netdevice_event+0x55f/0x1240 notifier_call_chain+0x5a/0xd0 call_netdevice_notifiers_info+0x39/0x90 unregister_netdevice_many_notify+0x63e/0x9d0 rtnl_dellink+0x16b/0x3a0 rtnetlink_rcv_msg+0x142/0x3f0 netlink_rcv_skb+0x50/0x100 netlink_unicast+0x242/0x390 netlink_sendmsg+0x1de/0x420 ____sys_sendmsg+0x2bd/0x320 ___sys_sendmsg+0x9a/0xe0 __sys_sendmsg+0x7a/0xd0 do_syscall_64+0x9e/0x1a0 entry_SYSCALL_64_after_hwframe+0x77/0x7f [3] unreferenced object 0xffff898081f597a0 (size 32): comm "ip", pid 1626, jiffies 4294719324 hex dump (first 32 bytes): 20 01 0d b8 00 02 00 00 00 00 00 00 00 00 00 01 ..... 21 49 61 83 80 89 ff ff 00 00 00 00 01 00 00 00 !Ia..... backtrace (crc fd9be911): [<00000000df89c55d>] __kmalloc_cache_noprof+0x1da/0x260 [<00000000ff2a1ddb>] mlxsw_sp_ipv6_addr_kvdl_index_get+0x281/0x340 [<000000009ddd445d>] mlxsw_sp_router_netdevice_event+0x47b/0x1240 [<00000000743e7757>] notifier_call_chain+0x5a/0xd0 [<000000007c7b9e13>] call_netdevice_notifiers_info+0x39/0x90 [<000000002509645d>] register_netdevice+0x5f7/0x7a0 [<00000000c2e7d2a9>] ip6gre_newlink_common.isra.0+0x65/0x130 [<0000000087cd6d8d>] ip6gre_newlink+0x72/0x120 [<000000004df7c7cc>] rtnl_newlink+0x471/0xa20 [<0000000057ed632a>] rtnetlink_rcv_msg+0x142/0x3f0 [<0000000032e0d5b5>] netlink_rcv_skb+0x50/0x100 [<00000000908bca63>] netlink_unicast+0x242/0x390 [<00000000cdbe1c87>] netlink_sendmsg+0x1de/0x420 [<0000000011db153e>] ____sys_sendmsg+0x2bd/0x320 [<000000003b6d53eb>] ___sys_sendmsg+0x9a/0xe0 [<00000000cae27c62>] __sys_sendmsg+0x7a/0xd0	5.5	More Details
CVE-2024-50141	In the Linux kernel, the following vulnerability has been resolved: ACPI: PRM: Find EFI_MEMORY_RUNTIME block for PRM handler and context PRMT needs to find the correct type of block to translate the PA-VA mapping for EFI runtime services. The issue arises because the PRMT is finding a block of type EFI_CONVENTIONAL_MEMORY, which is not appropriate for runtime services as described in Section 2.2.2 (Runtime Services) of the UEFI Specification [1]. Since the PRM handler is a type of runtime service, this causes an exception when the PRM handler is called. [Firmware Bug]: Unable to handle paging request in EFI runtime service WARNING: CPU: 22 PID: 4330 at drivers/firmware/efi/runtime-wrappers.c:341 __efi_queue_work+0x11c/0x170 Call trace: Let PRMT find a block with EFI_MEMORY_RUNTIME for PRM handler and PRM context. If no suitable block is found, a warning message will be printed, but the procedure continues to manage the next PRM handler. However, if the PRM handler is actually called without proper allocation, it would result in a failure during error handling. By using the correct memory types for runtime services, ensure that the PRM handler and the context are properly mapped in the virtual address space during runtime, preventing the paging request error. The issue is really that only memory that has been remapped for runtime by the firmware can be used by the PRM handler, and so the region needs to have the EFI_MEMORY_RUNTIME attribute. [rjw: Subject and changelog edits]	5.5	More Details
CVE-2024-50253	In the Linux kernel, the following vulnerability has been resolved: bpf: Check the validity of nr_words in bpf_iter_bits_new() Check the validity of nr_words in bpf_iter_bits_new(). Without this check, when multiplication overflow occurs for nr_bits (e.g., when nr_words = 0x0400-0001, nr_bits becomes 64), stack corruption may occur due to bpf_probe_read_kernel_common(..., nr_bytes = 0x2000-0008). Fix it by limiting the maximum value of nr_words to 511. The value is derived from the current implementation of BPF memory allocator. To ensure compatibility if the BPF memory allocator's size limitation changes in the future, use the helper bpf_mem_alloc_check_size() to check whether nr_bytes is too larger. And return -E2BIG instead of -ENOMEM for oversized nr_bytes.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50140	In the Linux kernel, the following vulnerability has been resolved: sched/core: Disable page allocation in task_tick_mm_cid() With KASAN and PREEMPT_RT enabled, calling task_work_add() in task_tick_mm_cid() may cause the following splat. [63.696416] BUG: sleeping function called from invalid context at kernel/locking/spinlock_rt.c:48 [63.696416] in_atomic(): 1, irqs_disabled(): 1, non_block: 0, pid: 610, name: modprobe [63.696416] preempt_count: 10001, expected: 0 [63.696416] RCU nest depth: 1, expected: 1 This problem is caused by the following call trace. sched_tick() [acquire rq->__lock] -> task_tick_mm_cid() -> task_work_add() -> __kasan_record_aux_stack() -> kasan_save_stack() -> stack_depot_save_flags() -> alloc_pages_mpol_noprof() -> __alloc_pages_noprof() -> get_page_from_freelist() -> rmqueue() -> rmqueue_pcplist() -> __rmqueue_pcplist() -> rmqueue_bulk() -> rt_spin_lock() The rq lock is a raw_spinlock_t. We can't sleep while holding it. IOW, we can't call alloc_pages() in stack_depot_save_flags(). The task_tick_mm_cid() function with its task_work_add() call was introduced by commit 223baf9d17f2 ("sched: Fix performance regression introduced by mm_cid") in v6.4 kernel. Fortunately, there is a kasan_record_aux_stack_noalloc() variant that calls stack_depot_save_flags() while not allowing it to allocate new pages. To allow task_tick_mm_cid() to use task_work without page allocation, a new TWAF_NO_ALLOC flag is added to enable calling kasan_record_aux_stack_noalloc() instead of kasan_record_aux_stack() if set. The task_tick_mm_cid() function is modified to add this new flag. The possible downside is the missing stack trace in a KASAN report due to new page allocation required when task_work_add_noallloc() is called which should be rare.	5.5	More Details
CVE-2024-50139	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: Fix shift-out-of-bounds bug Fix a shift-out-of-bounds bug reported by UBSAN when running VM with MTE enabled host kernel. UBSAN: shift-out-of-bounds in arch/arm64/kvm/sys_regs.c:1988:14 shift exponent 33 is too large for 32-bit type 'int' CPU: 26 UID: 0 PID: 7629 Comm: qemu-kvm Not tainted 6.12.0-rc2 #34 Hardware name: IEI NF5280R7/Mitchell MB, BIOS 00.00. 2024-10-12 09:28:54 10/14/2024 Call trace: dump_backtrace+0xa0/0x128 show_stack+0x20/0x38 dump_stack_lvl+0x74/0x90 dump_stack+0x18/0x28 __ubsan_handle_shift_out_of_bounds+0xf8/0x1e0 reset_clidr+0x10c/0x1c8 kvm_reset_sys_regs+0x50/0x1c8 kvm_reset_vcpu+0xec/0x2b0 __kvm_vcpu_set_target+0x84/0x158 kvm_vcpu_set_target+0x138/0x168 kvm_arch_vcpu_ioctl_vcpu_init+0x40/0x2b0 kvm_arch_vcpu_ioctl+0x28c/0x4b8 kvm_vcpu_ioctl+0x4bc/0x7a8 __arm64_sys_ioctl+0xb4/0x100 invoke_syscall+0x70/0x100 el0_svc_common.constprop.0+0x48/0xf0 do_el0_svc+0x24/0x38 el0_svc+0x3c/0x158 el0t_64_sync_handler+0x120/0x130 el0t_64_sync+0x194/0x198	5.5	More Details
CVE-2024-11079	A flaw was found in Ansible-Core. This vulnerability allows attackers to bypass unsafe content protections using the hostvars object to reference and execute templated content. This issue can lead to arbitrary code execution if remote data or module outputs are improperly templated within playbooks.	5.5	More Details
CVE-2024-50254	In the Linux kernel, the following vulnerability has been resolved: bpf: Free dynamically allocated bits in bpf_iter_bits_destroy() bpf_iter_bits_destroy() uses "kit->nr_bits <= 64" to check whether the bits are dynamically allocated. However, the check is incorrect and may cause a kmemleak as shown below: unreferenced object 0xffff88812628c8c0 (size 32): comm "swapper/0", pid 1, jiffies 4294727320 hex dump (first 32 bytes): b0 c1 55 f5 81 88 ff ff f0 f0 f0 f0 f0 f0 f0 f0 ..U..... f0 f0 f0 f0 f0 f0 f0 f0 00 00 00 00 00 00 00 00 ..... backtrace (crc 781e32cc): [<00000000c452b4ab>] kmemleak_alloc+0x4b/0x80 [<0000000004e09f80>] __kmalloc_node_noprof+0x480/0x5c0 [<00000000597124d6>] __alloc.isra.0+0x89/0xb0 [<000000004ebfffcd>] alloc_bulk+0x2af/0x720 [<00000000d9c10145>] prefill_mem_cache+0x7f/0xb0 [<00000000ff9738ff>] bpf_mem_alloc_init+0x3e2/0x610 [<000000008b616eac>] bpf_global_ma_init+0x19/0x30 [<00000000fc473efc>] do_one_initcall+0xd3/0x3c0 [<00000000ec81498c>] kernel_init_freeable+0x66a/0x940 [<00000000b119f72f>] kernel_init+0x20/0x160 [<00000000f11ac9a7>] ret_from_fork+0x3c/0x70 [<0000000004671da4>] ret_from_fork_asm+0x1a/0x30 That is because nr_bits will be set as zero in bpf_iter_bits_next() after all bits have been iterated. Fix the issue by setting kit->bit to kit->nr_bits instead of setting kit->nr_bits to zero when the iteration completes in bpf_iter_bits_next(). In addition, use "!nr_bits || bits >= nr_bits" to check whether the iteration is complete and still use "nr_bits > 64" to indicate whether bits are dynamically allocated. The "!nr_bits" check is necessary because bpf_iter_bits_new() may fail before setting kit->nr_bits, and this condition will stop the iteration early instead of accessing the zeroed or freed kit->bits. Considering the initial value of kit->bits is -1 and the type of kit->nr_bits is unsigned int, change the type of kit->nr_bits to int. The potential overflow problem will be handled in the following patch.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47435	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-50256	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_reject_ipv6: fix potential crash in nf_send_reset6() I got a syzbot report without a repro [1] crashing in nf_send_reset6() I think the issue is that dev->hard_header_len is zero, and we attempt later to push an Ethernet header. Use LL_MAX_HEADER, as other functions in net/ipv6/netfilter/nf_reject_ipv6.c. [1] skbuff: skb_under_panic: text:ffffffff89b1d008 len:74 put:14 head:ffff88803123aa00 data:ffff88803123a9f2 tail:0x3c end:0x140 dev:syz_tun kernel BUG at net/core/skbuff.c:206 ! Oops: invalid opcode: 0000 [#1] PREEMPT SMP KASAN PTI CPU: 0 UID: 0 PID: 7373 Comm: syz.1.568 Not tainted 6.12.0-rc2-syzkaller-00631-g6d858708d465 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 09/13/2024 RIP: 0010:skb_panic net/core/skbuff.c:206 [inline] RIP: 0010:skb_under_panic+0x14b/0x150 net/core/skbuff.c:216 Code: 0d 8d 48 c7 c6 60 a6 29 8e 48 8b 54 24 08 8b 0c 24 44 8b 44 24 04 4d 89 e9 50 41 54 41 57 41 56 e8 ba 30 38 02 48 83 c4 20 90 <0f> 0b 0f 1f 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 f3 RSP: 0018:ffffc900045269b0 EFLAGS: 00010282 RAX: 0000000000000088 RBX: dfffffc0000000000 RCX: cd66dacdc5d8e800 RDX: 0000000000000000 RSI: 0000000000000200 RDI: 0000000000000000 RBP: ffff88802d39a3d0 R08: ffffffff8174afec R09: 1ffff920008a4ccc R10: dfffffc0000000000 R11: fffff520008a4ccd R12: 0000000000000140 R13: ffff88803123aa00 R14: ffff88803123a9f2 R15: 000000000000003c FS: 00007fdbee5ff6c0(0000) GS:ffff8880b8600000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000000 CR3: 000000005d322000 CR4: 00000000003526f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> skb_push+0xe5/0x100 net/core/skbuff.c:2636 eth_header+0x38/0x1f0 net/ethernet/eth.c:83 dev_hard_header include/linux/netdevice.h:3208 [inline] nf_send_reset6+0xce6/0x1270 net/ipv6/netfilter/nf_reject_ipv6.c:358 nft_reject_inet_eval+0x3b9/0x690 net/netfilter/nft_reject_inet.c:48 expr_call_ops_eval net/netfilter/nf_tables_core.c:240 [inline] nft_do_chain+0x4ad/0x1da0 net/netfilter/nf_tables_core.c:288 nft_do_chain_inet+0x418/0x6b0 net/netfilter/nft_chain_filter.c:161 nf_hook_entry_hookfn include/linux/netfilter.h:154 [inline] nf_hook_slow+0xc3/0x220 net/netfilter/core.c:626 nf_hook include/linux/netfilter.h:269 [inline] NF_HOOK include/linux/netfilter.h:312 [inline] br_nf_pre_routing_ipv6+0x63e/0x770 net/bridge/br_netfilter_ipv6.c:184 nf_hook_entry_hookfn include/linux/netfilter.h:154 [inline] nf_hook_bridge_pre net/bridge/br_input.c:277 [inline] br_handle_frame+0x9fd/0x1530 net/bridge/br_input.c:424 __netif_receive_skb_core+0x13e8/0x4570 net/core/dev.c:5562 __netif_receive_skb_one_core net/core/dev.c:5666 [inline] __netif_receive_skb+0x12f/0x650 net/core/dev.c:5781 netif_receive_skb_internal net/core/dev.c:5867 [inline] netif_receive_skb+0x1e8/0x890 net/core/dev.c:5926 tun_rx_batched+0x1b7/0x8f0 drivers/net/tun.c:1550 tun_get_user+0x3056/0x47e0 drivers/net/tun.c:2007 tun_chr_write_iter+0x10d/0x1f0 drivers/net/tun.c:2053 new_sync_write fs/read_write.c:590 [inline] vfs_write+0xa6d/0xc90 fs/read_write.c:683 ksys_write+0x183/0x2b0 fs/read_write.c:736 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7fdbeeb7d1ff Code: 89 54 24 18 48 89 74 24 10 89 7c 24 08 e8 c9 8d 02 00 48 8b 54 24 18 48 8b 74 24 10 41 89 c0 8b 7c 24 08 b8 01 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 31 44 89 c7 48 89 44 24 08 e8 1c 8e 02 00 48 RSP: 002b:00007fdbee5ff000 EFLAGS: 00000293 ORIG_RAX: 0000000000000001 RAX: ffffffffffffffda RBX: 00007fdbeed36058 RCX: 00007fdbeeb7d1ff RDX: 000000000000008e RSI: 0000000020000040 RDI: 00000000000000c8 RBP: 00007fdbeebf12be R08: 0000000 ---truncated---	5.5	More Details
CVE-2024-50259	In the Linux kernel, the following vulnerability has been resolved: netdevsim: Add trailing zero to terminate the string in nsim_nexthop_bucket_activity_write() This was found by a static analyzer. We should not forget the trailing zero after copy_from_user() if we will further do some string operations, sscanf() in this case. Adding a trailing zero will ensure that the function performs properly.	5.5	More Details
CVE-2024-47446	After Effects versions 23.6.9, 24.6.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-47445	After Effects versions 23.6.9, 24.6.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47444	After Effects versions 23.6.9, 24.6.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-49512	InDesign Desktop versions ID18.5.3, ID19.5 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-45147	Bridge versions 13.0.9, 14.1.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-50258	In the Linux kernel, the following vulnerability has been resolved: net: fix crash when config small gso_max_size/gso_ipv4_max_size Config a small gso_max_size/gso_ipv4_max_size will lead to an underflow in sk_dst_gso_max_size(), which may trigger a BUG_ON crash, because sk->sk_gso_max_size would be much bigger than device limits. Call Trace: tcp_write_xmit tso_segs = tcp_init_tso_segs(skb, mss_now); tcp_set_skb_tso_segs tcp_skb_pcount_set // skb->len = 524288, mss_now = 8 // u16 tso_segs = 524288/8 = 65535 -> 0 tso_segs = DIV_ROUND_UP(skb->len, mss_now) BUG_ON(!tso_segs) Add check for the minimum value of gso_max_size and gso_ipv4_max_size.	5.5	More Details
CVE-2021-27703	Sercomm Model Etisalat Model S3- AC2100 is affected by Cross Site Scripting (XSS) via the firmware update page.	5.4	More Details
CVE-2024-43437	A flaw was found in moodle. Insufficient sanitizing of data when performing a restore could result in a cross-site scripting (XSS) risk from malicious backup files.	5.4	More Details
CVE-2024-35146	IBM Maximo Application Suite - Monitor Component 8.10.11, 8.11.8, and 9.0.0 is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	5.4	More Details
CVE-2024-43439	A flaw was found in moodle. H5P error messages require additional sanitizing to prevent a reflected cross-site scripting (XSS) risk.	5.4	More Details
CVE-2024-51032	A Cross-site Scripting (XSS) vulnerability in manage_recipient.php of Sourcecodester Toll Tax Management System 1.0 allows remote authenticated users to inject arbitrary web scripts via the "owner" input field.	5.4	More Details
CVE-2024-11021	Webopac from Grand Vice info has Stored Cross-site Scripting vulnerability. Remote attackers with regular privileges can inject arbitrary JavaScript code into the server. When users visit the compromised page, the code is automatically executed in their browser.	5.4	More Details
CVE-2024-52312	Due to inconsistent authorization permissions, data.all may allow an external actor with an authenticated account to perform restricted operations against DataSets and Environments.	5.4	More Details
CVE-2024-51031	A Cross-site Scripting (XSS) vulnerability in manage_account.php in Sourcecodester Cab Management System 1.0 allows remote authenticated users to inject arbitrary web scripts via the "First Name," "Middle Name," and "Last Name" fields.	5.4	More Details
CVE-2024-28730	Cross Site Scripting vulnerability in DLink DWR 2000M 5G CPE With Wifi 6 Ax1800 and Dlink DWR 5G CPE DWR-2000M_1.34ME allows a local attacker to obtain sensitive information via the file upload feature of the VPN configuration module.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49524	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by an attacker to execute arbitrary code in the context of the victim's browser session. By manipulating a DOM element through a crafted URL or user input, the attacker can inject malicious scripts that run when the page is rendered. This type of attack requires user interaction, as the victim would need to access a manipulated URL or provide specific input to trigger the vulnerability.	5.4	More Details
CVE-2024-46965	The DS allvideo.downloader.browser (aka Fast Video Downloader: Browser) application through 1.6-RC1 for Android allows an attacker to execute arbitrary JavaScript code via the allvideo.downloader.browser.DefaultBrowserActivity component.	5.4	More Details
CVE-2024-10318	A session fixation issue was discovered in the NGINX OpenID Connect reference implementation, where a nonce was not checked at login time. This flaw allows an attacker to fix a victim's session to an attacker-controlled account. As a result, although the attacker cannot log in as the victim, they can force the session to associate it with the attacker-controlled account, leading to potential misuse of the victim's session.	5.4	More Details
CVE-2024-10790	The Admin and Site Enhancements (ASE) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 7.5.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with custom-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file. This feature must be enabled, and for specific roles in order to be exploitable.	5.4	More Details
CVE-2024-30140	HCL BigFix Compliance is affected by unvalidated redirects and forwards. The HOST header can be manipulated by an attacker and as a result, it can poison the web cache and provide back to users being served the page.	5.4	More Details
CVE-2023-47543	An authorization bypass through user-controlled key vulnerability [CWE-639] in Fortinet FortiPortal version 7.0.0 through 7.0.3 allows an authenticated attacker to interact with ressources of other organizations via HTTP or HTTPS requests.	5.4	More Details
CVE-2024-50637	UnoPim 0.1.3 and below is vulnerable to Cross Site Scripting (XSS) in the Create User function. This allows attackers to perform XSS via an SVG document, which can be used to steal cookies.	5.4	More Details
CVE-2024-51026	The NetAdmin IAM system (version 4.0.30319) has a Cross Site Scripting (XSS) vulnerability in the /BalloonSave.ashx endpoint, where it is possible to inject a malicious payload into the Content= field.	5.4	More Details
CVE-2024-20540	A vulnerability in the web-based management interface of Cisco Unified Contact Center Management Portal (Unified CCMP) could allow an authenticated, remote attacker with low privileges to conduct a stored cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into a specific page 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 Supervisor role on an affected device.	5.4	More Details
CVE-2020-11918	An issue was discovered in Siime Eye 14.1.00000001.3.330.0.0.3.14. When a backup file is created through the web interface, information on all users, including passwords, can be found in cleartext in the backup file. An attacker capable of accessing the web interface can create the backup file.	5.4	More Details
CVE-2024-49523	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-51489	Ampache is a web based audio/video streaming application and file manager. The current implementation of token parsing does not adequately validate CSRF tokens when users send messages to one another. This vulnerability could be exploited to forge CSRF attacks, allowing an attacker to send messages to any user, including administrators, if they interact with a malicious request. This issue has been addressed in version 7.0.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50810	hopetree izone lts c011b48 contains a Cross Site Scripting (XSS) vulnerability in the article comment function. In \apps\comment\views.py, AddCommintView() does not securely filter user input and renders it directly to the frontend page through templates.	5.4	More Details
CVE-2024-51987	Duende.AccessTokenManagement.OpenIdConnect is a set of .NET libraries that manage OAuth and OpenId Connect access tokens. HTTP Clients created by `AddUserAccessTokenHttpClient` may use a different user's access token after a token refresh occurs. This occurs because a refreshed token will be captured in pooled `HttpClient` instances, which may be used by a different user. Instead of using `AddUserAccessTokenHttpClient` to create an `HttpClient` that automatically adds a managed token to outgoing requests, you can use the `HttpConext.GetUserAccessTokenAsync` extension method or the `IUserTokenManagementService.GetAccessTokenAsync` method. This issue is fixed in Duende.AccessTokenManagement.OpenIdConnect 3.0.1. All users are advised to upgrade. There are no known workarounds for this vulnerability.	5.4	More Details
CVE-2024-51488	Ampache is a web based audio/video streaming application and file manager. The current implementation of token parsing does not adequately validate CSRF tokens when users delete messages. This vulnerability could be exploited to forge CSRF attacks, allowing an attacker to delete messages to any user, including administrators, if they interact with a malicious request. This issue has been addressed in version 7.0.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	5.4	More Details
CVE-2024-20514	A vulnerability in the web-based management interface of Cisco Evolved Programmable Network Manager (EPNM) and Cisco Prime Infrastructure could allow an authenticated, low-privileged, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into a specific page 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-2024-20504	A vulnerability in the web-based management interface of Cisco AsyncOS Software for Cisco Secure Email and Web Manager, Secure Email Gateway, and Secure Web Appliance could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	5.4	More Details
CVE-2024-10535	The Video Gallery for WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the remove_unused_thumbnails() function in all versions up to, and including, 1.31. This makes it possible for unauthenticated attackers to delete thumbnails in the video-wc-gallery-thumb directory.	5.3	More Details
CVE-2024-6626	The EleForms – All In One Form Integration including DB for Elementor plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on several functions in all versions up to, and including, 2.9.9.9. This makes it possible for unauthenticated attackers to view form submissions.	5.3	More Details
CVE-2024-52043	Generation of Error Message Containing Sensitive Information in HumHub GmbH & Co. KG - HumHub on Linux allows: Excavation (user enumeration).This issue affects all released HumHub versions: through 1.16.2.	5.3	More Details
CVE-2024-10916	A vulnerability classified as problematic has been found in D-Link DNS-320, DNS-320LW, DNS-325 and DNS-340L up to 20241028. This affects an unknown part of the file /xml/info.xml of the component HTTP GET Request Handler. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2024-48075	A Heap buffer overflow in the server-site handshake implementation in Real Time Logic SharkSSL from 09/09/24 and earlier allows a remote attacker to trigger a Denial-of-Service via a malformed TLS Client Key Exchange message.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26011	A missing authentication for critical function in Fortinet FortiManager version 7.4.0 through 7.4.2, 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.14, FortiPAM version 1.2.0, 1.1.0 through 1.1.2, 1.0.0 through 1.0.3, FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.9, 7.0.0 through 7.0.17, 2.0.0 through 2.0.14, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7, FortiSwitchManager version 7.2.0 through 7.2.3, 7.0.0 through 7.0.3, FortiPortal version 6.0.0 through 6.0.14, FortiOS version 7.4.0 through 7.4.3, 7.2.0 through 7.2.7, 7.0.0 through 7.0.14, 6.4.0 through 6.4.15, 6.2.0 through 6.2.16, 6.0.0 through 6.0.18 allows attacker to execute unauthorized code or commands via specially crafted packets.	5.3	More Details
CVE-2024-20445	A vulnerability in the web UI of Cisco Desk Phone 9800 Series, Cisco IP Phone 7800 and 8800 Series, and Cisco Video Phone 8875 could allow an unauthenticated, remote attacker to access sensitive information on an affected device. This vulnerability is due to improper storage of sensitive information within the web UI of Session Initiation Protocol (SIP)-based phone loads. An attacker could exploit this vulnerability by browsing to the IP address of a device that has Web Access enabled. A successful exploit could allow the attacker to access sensitive information, including incoming and outgoing call records. Note: Web Access is disabled by default.	5.3	More Details
CVE-2024-20371	A vulnerability in the access control list (ACL) programming of Cisco Nexus 3550-F Switches could allow an unauthenticated, remote attacker to send traffic that should be blocked to the management interface of an affected device. This vulnerability exists because ACL deny rules are not properly enforced at the time of device reboot. An attacker could exploit this vulnerability by attempting to send traffic to the management interface of an affected device. A successful exploit could allow the attacker to send traffic to the management interface of the affected device.	5.3	More Details
CVE-2024-49405	Improper authentication in Private Info in Samsung Pass in prior to version 4.4.04.7 allows physical attackers to access sensitive information in a specific scenario.	5.3	More Details
CVE-2024-43435	A flaw was found in moodle. Insufficient capability checks make it possible for users with access to restore glossaries in courses to restore them into the global site glossary.	5.3	More Details
CVE-2024-46889	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 3). The affected application uses hard-coded cryptographic key material to obfuscate configuration files. This could allow an attacker to learn that cryptographic key material through reverse engineering of the application binary and decrypt arbitrary backup files.	5.3	More Details
CVE-2024-49395	In mutt and neomutt, PGP encryption does not use the --hidden-recipient mode which may leak the Bcc email header field by inferring from the recipients info.	5.3	More Details
CVE-2024-47586	SAP NetWeaver Application Server for ABAP and ABAP Platform allows an unauthenticated attacker to send a maliciously crafted http request which could cause a null pointer dereference in the kernel. This dereference will result in the system crashing and rebooting, causing the system to be temporarily unavailable. There is no impact on Confidentiality or Integrity.	5.3	More Details
CVE-2024-10779	The Cowidgets – Elementor Addons plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.2.0 via the 'ce_template' shortcode due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from private or draft posts created by Elementor that they should not have access to.	5.3	More Details
CVE-2024-39281	The command ctl_persistent_reserve_out allows the caller to specify an arbitrary size which will be passed to the kernel's memory allocator.	5.3	More Details
CVE-2024-47592	SAP NetWeaver AS Java allows an unauthenticated attacker to brute force the login functionality in order to identify the legitimate user IDs. This has an impact on confidentiality but not on integrity or availability.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8756	The Quform - WordPress Form Builder plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.20.0 via the 'saveUploadedFile' function. This makes it possible for unauthenticated attackers to extract sensitive data, such as Personally Identifiable Information, from files uploaded by users. Files uploaded via forms created before version 2.21.0 will remain vulnerable to exposure after upgrading. To fully patch the plugin, site administrators should download any previously uploaded files, delete previously existing files and forms, and create the forms again after upgrading to version 2.21.0.	5.3	More Details
CVE-2024-49394	In mutt and neomutt the In-Reply-To email header field is not protected by cryptographic signing which allows an attacker to reuse an unencrypted but signed email message to impersonate the original sender.	5.3	More Details
CVE-2024-43429	A flaw was found in moodle. Some hidden user profile fields are visible in gradebook reports, which could result in users without the "view hidden user fields" capability having access to the information.	5.3	More Details
CVE-2024-46891	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 3). The affected application does not properly restrict the size of generated log files. This could allow an unauthenticated remote attacker to trigger a large amount of logged events to exhaust the system's resources and create a denial of service condition.	5.3	More Details
CVE-2024-43430	A flaw was found in moodle. External API access to Quiz can override contained insufficient access control.	5.3	More Details
CVE-2024-43433	A flaw was found in moodle. Matrix room membership and power levels are incorrectly applied and revoked for suspended Moodle users.	5.3	More Details
CVE-2024-50313	A vulnerability has been identified in Mendix Runtime V10 (All versions < V10.16.0 only if the basic authentication mechanism is used by the application), Mendix Runtime V10.12 (All versions < V10.12.7 only if the basic authentication mechanism is used by the application), Mendix Runtime V10.6 (All versions < V10.6.15 only if the basic authentication mechanism is used by the application), Mendix Runtime V8 (All versions), Mendix Runtime V9 (All versions < V9.24.29 only if the basic authentication mechanism is used by the application). The basic authentication implementation of affected applications contains a race condition vulnerability which could allow unauthenticated remote attackers to circumvent default account lockout measures.	5.3	More Details
CVE-2024-30133	HCL Traveler for Microsoft Outlook (HTMO) is susceptible to a control flow vulnerability. The application does not sufficiently manage its control flow during execution, creating conditions in which the control flow can be modified in unexpected ways.	5.3	More Details
CVE-2024-43432	A flaw was found in moodle. The cURL wrapper in Moodle strips HTTPAUTH and USERPWD headers during emulated redirects, but retains other original request headers, so HTTP authorization header information could be unintentionally sent in requests to redirect URLs.	5.3	More Details
CVE-2024-49401	Improper input validation in Settings Suggestions prior to SMR Nov-2024 Release 1 allows local attackers to launch privileged activities.	5.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-52288	libosdp is an implementation of IEC 60839-11-5 OSDP (Open Supervised Device Protocol) and provides a C library with support for C++, Rust and Python3. In affected versions an unexpected `REPLY_CCRYPT` or `REPLY_RMAC_I` may be introduced into an active stream when they should not be. Once RMAC_I message can be sent during a session, attacker with MITM access to the communication may intercept the original RMAC_I reply and save it. While the session continues, the attacker will record all of the replies and save them, till capturing the message to be replied (can be detected by ID, length or time based on inspection of visual activity next to the reader) Once attacker captures a session with the message to be replayed, he stops resetting the connection and waits for signal to perform the replay to of the PD to CP message (ex: by signaling remotely to the MIMT device or setting a specific timing). In order to replay, the attacker will craft a specific RMAC_I message in the proper seq of the execution, which will result in reverting the RMAC to the beginning of the session. At that phase - attacker can replay all the messages from the beginning of the session. This issue has been addressed in commit `298576d9` which is included in release version 3.0.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.1	More Details
CVE-2024-32116	Multiple relative path traversal vulnerabilities [CWE-23] in Fortinet FortiManager version 7.4.0 through 7.4.2 and before 7.2.5, FortiAnalyzer version 7.4.0 through 7.4.2 and before 7.2.5 and FortiAnalyzer-BigData version 7.4.0 and before 7.2.7 allows a privileged attacker to delete files from the underlying filesystem via crafted CLI requests.	5.1	More Details
CVE-2024-51750	Element is a Matrix web client built using the Matrix React SDK. A malicious homeserver can send invalid messages over federation which can prevent Element Web and Desktop from rendering single messages or the entire room containing them. This was patched in Element Web and Desktop 1.11.85.	5.0	More Details
CVE-2024-9843	A buffer over-read in Ivanti Secure Access Client before 22.7R4 allows a local unauthenticated attacker to cause a denial of service.	5.0	More Details
CVE-2024-50378	Airflow versions before 2.10.3 have a vulnerability that allows authenticated users with audit log access to see sensitive values in audit logs which they should not see. When sensitive variables were set via airflow CLI, values of those variables appeared in the audit log and were stored unencrypted in the Airflow database. While this risk is limited to users with audit log access, it is recommended to upgrade to Airflow 2.10.3 or a later version, which addresses this issue. Users who previously used the CLI to set secret variables should manually delete entries with those variables from the log table.	4.9	More Details
CVE-2024-47905	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.3 and Ivanti Policy Secure before version 22.7R1.2 allows a remote authenticated attacker with admin privileges to cause a denial of service.	4.9	More Details
CVE-2024-9874	The Poll Maker – Versus Polls, Anonymous Polls, Image Polls plugin for WordPress is vulnerable to time-based SQL Injection via the ‘orderby’ parameter in all versions up to, and including, 5.4.6 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2024-47909	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.3 and Ivanti Policy Secure before version 22.7R1.2 allows a remote authenticated attacker with admin privileges to cause a denial of service.	4.9	More Details
CVE-2024-52314	A data.all admin team member who has access to the customer-owned AWS Account where data.all is deployed may be able to extract user data from data.all application logs in data.all via CloudWatch log scanning for particular operations that interact with customer producer teams data.	4.9	More Details
CVE-2024-32117	An improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability [CWE-22] in Fortinet FortiManager version 7.4.0 through 7.4.2 and below 7.2.5, FortiAnalyzer version 7.4.0 through 7.4.2 and below 7.2.5 & FortiAnalyzer-BigData version 7.4.0 and below 7.2.7 allows a privileged attacker to read arbitrary files from the underlying system via crafted HTTP or HTTPs requests.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46892	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 3). The affected application does not properly invalidate sessions when the associated user is deleted or disabled or their permissions are modified. This could allow an authenticated attacker to continue performing malicious actions even after their user account has been disabled.	4.9	More Details
CVE-2024-51720	An insufficient entropy vulnerability in the SecuSUITE Secure Client Authentication (SCA) Server of SecuSUITE versions 5.0.420 and earlier could allow an attacker to potentially enroll an attacker-controlled device to the victim’s account and telephone number.	4.8	More Details
CVE-2024-10027	The WP Booking Calendar WordPress plugin before 10.6.3 does not sanitise and escape some of its Widgets 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-2024-8378	The Safe SVG WordPress plugin before 2.2.6 has its sanitisation code is only running for paths that call wp_handle_upload, but not for example for code that uses wp_handle_sideload which is often used to upload attachments via raw POST data.	4.8	More Details
CVE-2024-20539	A vulnerability in the web-based management interface of Cisco ISE could allow an authenticated, remote attacker to conduct a stored XSS attack against a user of the interface. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker would need valid administrative credentials on an affected device.	4.8	More Details
CVE-2024-20534	A vulnerability in the web UI of Cisco Desk Phone 9800 Series, Cisco IP Phone 6800, 7800, and 8800 Series, and Cisco Video Phone 8875 with Cisco Multiplatform Firmware could allow an authenticated, remote attacker to conduct stored cross-site scripting (XSS) attacks against users. This vulnerability exists because the web UI of an affected device does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Note: To exploit this vulnerability, Web Access must be enabled on the phone and the attacker must have Admin credentials on the device. Web Access is disabled by default.	4.8	More Details
CVE-2024-9835	The RSS Feed Widget WordPress plugin before 3.0.1 does not escape the $_SERVER['REQUEST_URI'] parameter before outputting it back in an attribute, which could lead to Reflected Cross-Site Scripting in old web browsers	4.8	More Details
CVE-2024-51190	TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices contain a Store Cross-site scripting (XSS) vulnerability via the ptRule_ApplicationName_1.1.6.0.0 parameter on the /special_ap.htm page.	4.8	More Details
CVE-2024-51189	TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices contain a Store Cross-site scripting (XSS) vulnerability via the macList_Name_1.1.1.0.0 parameter on the /filters.htm page.	4.8	More Details
CVE-2024-51188	TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices contain a Store Cross-site scripting (XSS) vulnerability via the vsRule_VirtualServerName_1.1.10.0.0 parameter on the /virtual_server.htm page.	4.8	More Details
CVE-2024-51187	TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices contain a Store Cross-site scripting (XSS) vulnerability via the firewallRule_Name_1.1.1.0.0 parameter on the /firewall_setting.htm page.	4.8	More Details
CVE-2024-45087	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	4.8	More Details
CVE-2024-51054	A Cross Site Scriptng (XSS) vulnerability was found in /omrs/admin/search.php in PHPGurukul Online Marriage Registration System 1.0, which allows remote attackers to execute arbitrary code via the "searchdata" POST request parameter.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50991	A Cross Site Scripting (XSS) vulnerability was found in /ums-sp/admin/registered-users.php in PHPGurukul User Management System v1.0, which allows remote attackers to execute arbitrary code via the "fname" POST request parameter	4.8	More Details
CVE-2024-7879	The WP ULike WordPress plugin before 4.7.5 does not sanitise and escape some of its settings, which could allow high privilege users such as editors to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details
CVE-2024-20533	A vulnerability in the web UI of Cisco Desk Phone 9800 Series, Cisco IP Phone 6800, 7800, and 8800 Series, and Cisco Video Phone 8875 with Cisco Multiplatform Firmware could allow an authenticated, remote attacker to conduct stored cross-site scripting (XSS) attacks against users. This vulnerability exists because the web UI of an affected device does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Note: To exploit this vulnerability, Web Access must be enabled on the phone and the attacker must have Admin credentials on the device. Web Access is disabled by default.	4.8	More Details
CVE-2024-50260	In the Linux kernel, the following vulnerability has been resolved: sock_map: fix a NULL pointer dereference in sock_map_link_update_prog() The following race condition could trigger a NULL pointer dereference: sock_map_link_detach(): sock_map_link_update_prog(): mutex_lock(&sockmap_mutex); ... sockmap_link->map = NULL; mutex_unlock(&sockmap_mutex); mutex_lock(&sockmap_mutex); ... sock_map_prog_link_lookup(sockmap_link->map); mutex_unlock(&sockmap_mutex); <continue> Fix it by adding a NULL pointer check. In this specific case, it makes no sense to update a link which is being released.	4.7	More Details
CVE-2024-11101	A vulnerability was found in 1000 Projects Beauty Parlour Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/search-invoices.php. The manipulation of the argument searchdata leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2024-30141	HCL BigFix Compliance is vulnerable to the generation of error messages containing sensitive information. Detailed error messages can provide enticement information or expose information about its environment, users, or associated data.	4.7	More Details
CVE-2024-10947	A vulnerability classified as critical was found in Guangzhou Tuchuang Computer Software Development Interlib Library Cluster Automation Management System up to 2.0.1. This vulnerability affects unknown code of the file /interlib/order/BatchOrder?cmdACT=admin_order&xsl=adminOrder_OrderList.xsl. The manipulation of the argument bookrecno leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-10946	A vulnerability classified as critical has been found in Guangzhou Tuchuang Computer Software Development Interlib Library Cluster Automation Management System up to 2.0.1. This affects an unknown part of the file /interlib/admin/SysLib?cmdACT=inputLIBCODE&mod=batchXSL&xsl=editLIBCODE.xsl&libcodes=&ROWID=. The manipulation of the argument sql leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-47588	In SAP NetWeaver Java (Software Update Manager 1.1), under certain conditions when a software upgrade encounters errors, credentials are written in plaintext to a log file. An attacker with local access to the server, authenticated as a non-administrative user, can acquire the credentials from the logs. This leads to a high impact on confidentiality, with no impact on integrity or availability.	4.7	More Details
CVE-2024-11058	A vulnerability was found in CodeAstro Real Estate Management System up to 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /aboutedit.php of the component About Us Page. 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.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27701	SOCIFI Socifi Guest wifi as SAAS is affected by Cross Site Request Forgery (CSRF) via the Socifi wifi portal. The application does not contain a CSRF token and request validation. An attacker can Add/Modify any random user data by sending a crafted CSRF request.	4.7	More Details
CVE-2024-11124	A vulnerability has been found in TimGeyssens UIOMatic 5 and classified as critical. This vulnerability affects unknown code of the file /src/UIOMatic/wwwroot/backoffice/resources/uioMaticObject.r. The manipulation leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2024-51157	07FLYCMS V1.3.9 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component http://erp.07fly.net:80/oa/OaSchedule/add.html.	4.7	More Details
CVE-2024-10999	A vulnerability classified as problematic has been found in CodeAstro Real Estate Management System 1.0. Affected is an unknown function of the file /aboutadd.php of the component About Us Page. The manipulation of the argument aimage leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2024-11000	A vulnerability classified as problematic was found in CodeAstro Real Estate Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /aboutedit.php of the component About Us Page. The manipulation of the argument aimage leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2024-50174	In the Linux kernel, the following vulnerability has been resolved: drm/panthor: Fix race when converting group handle to group object XArray provides it's own internal lock which protects the internal array when entries are being simultaneously added and removed. However there is still a race between retrieving the pointer from the XArray and incrementing the reference count. To avoid this race simply hold the internal XArray lock when incrementing the reference count, this ensures there cannot be a racing call to xa_erase().	4.7	More Details
CVE-2024-50183	In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Ensure DA_ID handling completion before deleting an NPIV instance Deleting an NPIV instance requires all fabric ndlps to be released before an NPIV's resources can be torn down. Failure to release fabric ndlps beforehand opens kref imbalance race conditions. Fix by forcing the DA_ID to complete synchronously with usage of wait_queue.	4.7	More Details
CVE-2024-50192	In the Linux kernel, the following vulnerability has been resolved: irqchip/gic-v4: Don't allow a VMOVP on a dying VPE Kunkun Jiang reported that there is a small window of opportunity for userspace to force a change of affinity for a VPE while the VPE has already been unmapped, but the corresponding doorbell interrupt still visible in /proc/irq/. Plug the race by checking the value of vmapp_count, which tracks whether the VPE is mapped ot not, and returning an error in this case. This involves making vmapp_count common to both GICv4.1 and its v4.0 ancestor.	4.7	More Details
CVE-2024-49403	Improper access control in Samsung Voice Recorder prior to version 21.5.40.37 allows physical attackers to access recording files on the lock screen.	4.6	More Details
CVE-2019-20469	An issue was discovered on One2Track 2019-12-08 devices. Confidential information is needlessly stored on the smartwatch. Audio files are stored in .amr format, in the audior directory. An attacker who has physical access can retrieve all audio files by connecting via a USB cable.	4.6	More Details
CVE-2024-49402	Improper input validation in Dressroom prior to SMR Nov-2024 Release 1 allow physical attackers to access data across multiple user profiles.	4.6	More Details
CVE-2024-29075	Active debug code vulnerability exists in Mesh Wi-Fi router RP562B firmware version v1.0.2 and earlier. If this vulnerability is exploited, a network-adjacent authenticated attacker may obtain or alter the settings of the device .	4.6	More Details
CVE-2024-34674	Improper access control in Contacts prior to SMR Nov-2024 Release 1 allows physical attackers to access data across multiple user profiles.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49407	Improper access control in Samsung Flow prior to version 4.9.15.7 allows physical attackers to access data across multiple user profiles.	4.6	More Details
CVE-2024-8882	A buffer overflow vulnerability in the CGI program in the Zyxel GS1900-48 switch firmware version V2.80(AAHN.1)C0 and earlier could allow an authenticated, LAN-based attacker with administrator privileges to cause denial of service (DoS) conditions via a crafted URL.	4.5	More Details
CVE-2024-34676	Out-of-bounds write in parsing subtitle file in libsubextractor.so prior to SMR Nov-2024 Release 1 allows local attackers to cause memory corruption. User interaction is required for triggering this vulnerability.	4.4	More Details
CVE-2024-51785	Server-Side Request Forgery (SSRF) vulnerability in I Thirteen Web Solution Responsive Filterable Portfolio allows Server Side Request Forgery.This issue affects Responsive Filterable Portfolio: from n/a through 1.0.22.	4.4	More Details
CVE-2024-11111	Inappropriate implementation in Autofill in Google Chrome prior to 131.0.6778.69 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2024-10770	The Envo Extra plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.9.3 via the 'elementor-template' shortcode due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from private or draft posts created by Elementor that they should not have access to.	4.3	More Details
CVE-2024-11123	A vulnerability, which was classified as problematic, was found in 上海灵当信息科技有限公司 Lingdang CRM up to 8.6.4.3. This affects an unknown part of the file /crm/data/pdf.php. The manipulation of the argument url with the input ../config.inc.php leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-10669	The Countdown Timer block – Display the event's date into a timer. plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.2.4 via the [ctb] shortcode due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from password protected, private, or draft posts that they should not have access to.	4.3	More Details
CVE-2024-10695	The Futurio Extra plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 2.0.13 via the 'elementor-template' shortcode due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from private or draft posts that they should not have access to.	4.3	More Details
CVE-2024-10693	The SKT Addons for Elementor plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 3.3 via the Unfold widget due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from private or draft posts created by Elementor that they should not have access to.	4.3	More Details
CVE-2024-10543	The Tumult Hype Animations plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the hypeanimations_getcontent function in all versions up to, and including, 1.9.14. This makes it possible for authenticated attackers, with Subscriber-level access and above, to retrieve animation information.	4.3	More Details
CVE-2024-28731	Cross Site Request Forgery vulnerability in DLink DWR 2000M 5G CPE With Wifi 6 Ax1800 and Dlink DWR 5G CPE DWR-2000M_1.34ME allows a local attacker to obtain sensitive information via the Port forwarding option.	4.3	More Details
CVE-2024-10971	Improper access control in the Password History feature in Devolutions DVLS 2024.3.6 and earlier allows a malicious authenticated user to obtain sensitive data via faulty permission.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46948	Northern.tech Mender before 3.6.5 and 3.7.x before 3.7.5 has Incorrect Access Control.	4.3	More Details
CVE-2024-47593	SAP NetWeaver Application Server ABAP allows an unauthenticated attacker with network access to read files from the server, which otherwise would be restricted.This attack is possible only if a Web Dispatcher or some sort of Proxy Server is in use and the file in question was previously opened or downloaded in an application based on SAP GUI for HTML Technology. This will not compromise the application's integrity or availability.	4.3	More Details
CVE-2024-52313	An authenticated data.all user is able to manipulate a getDataset query to fetch additional information regarding the parent Environment resource that the user otherwise would not able to fetch by directly querying the object via getEnvironment in data.all.	4.3	More Details
CVE-2024-11073	A vulnerability classified as problematic has been found in SourceCodester Hospital Management System 1.0. This affects an unknown part of the file /vm/patient/delete-account.php. The manipulation of the argument id leads to improper authorization. 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-2024-33510	An improper neutralization of special elements in output used by a downstream component ('Injection') vulnerability [CWE-74] in FortiOS version 7.4.3 and below, version 7.2.8 and below, version 7.0.16 and below; FortiProxy version 7.4.3 and below, version 7.2.9 and below, version 7.0.16 and below; FortiSASE version 24.2.b SSL-VPN web user interface may allow a remote unauthenticated attacker to perform phishing attempts via crafted requests.	4.3	More Details
CVE-2024-10953	An authenticated data.all user is able to perform mutating UPDATE operations on persisted Notification records in data.all for group notifications that their user is not a member of.	4.3	More Details
CVE-2024-20476	A vulnerability in the web-based management interface of Cisco ISE could allow an authenticated, remote attacker to bypass the authorization mechanisms for specific file management functions. This vulnerability is due to lack of server-side validation of Administrator permissions. An attacker could exploit this vulnerability by submitting a crafted HTTP request to an affected system. A successful exploit could allow the attacker to upload files to a location that should be restricted. To exploit this vulnerability, an attacker would need valid Read-Only Administrator credentials.	4.3	More Details
CVE-2024-20487	A vulnerability in the web-based management interface of Cisco ISE could allow an authenticated, remote attacker to conduct a stored 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.	4.3	More Details
CVE-2024-10352	The Magical Addons For Elementor plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.2.4 via the get_content_type function in includes/widgets/content-reveal.php. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive private, pending, and draft template data.	4.3	More Details
CVE-2024-20507	A vulnerability in the logging subsystem of Cisco Meeting Management could allow an authenticated, remote attacker to view sensitive information in clear text on an affected system. This vulnerability is due to improper storage of sensitive information within the web-based management interface of an affected device. An attacker could exploit this vulnerability by logging in to the web-based management interface. A successful exploit could allow the attacker to view sensitive data that is stored on the affected device.	4.3	More Details
CVE-2024-52032	Mattermost versions 10.0.x <= 10.0.0 and 9.11.x <= 9.11.2 fail to properly query ElasticSearch when searching for the channel name in channel switcher which allows an attacker to get private channels names of channels that they are not a member of, when Elasticsearch v8 was enabled.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10588	The Debug Tool plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the info() function in all versions up to, and including, 2.2. This makes it possible for authenticated attackers, with subscriber-level access and above, to obtain information from phpinfo(). When WP_DEBUG is enabled, this can be exploited by unauthenticated users as well.	4.3	More Details
CVE-2024-10667	The Content Slider Block plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 3.1.5 via the [csb] shortcode due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from password protected, private, or draft posts that they should not have access to.	4.3	More Details
CVE-2024-10688	The Attesa Extra plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.4.2 via the 'attesa-template' shortcode due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from password protected, private, or draft posts that they should not have access to.	4.3	More Details
CVE-2024-50561	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.2), RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2) (All versions < V8.2), SCALANCE M804PB (6GK5804-0AP00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1AA00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1BA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2) (All versions < V8.2), SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) (All versions < V8.2), SCALANCE M874-2 (6GK5874-2AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 (6GK5874-3AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2) (All versions < V8.2), SCALANCE M876-3 (6GK5876-3AA02-2BA2) (All versions < V8.2), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.2), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.2), SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) (All versions < V8.2), SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) (All versions < V8.2), SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1) (All versions < V8.2), SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1) (All versions < V8.2), SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) (All versions < V8.2), SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1) (All versions < V8.2), SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1) (All versions < V8.2), SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1) (All versions < V8.2), SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) (All versions < V8.2), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.2), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All versions < V8.2), SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2) (All versions < V8.2). Affected devices do not properly sanitize the filenames before uploading. This could allow an authenticated remote attacker to compromise of integrity of the system.	4.3	More Details
CVE-2024-21994	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.9 are susceptible to a Denial of Service (DoS) vulnerability. Successful exploit by an authenticated attacker could lead to a service crash.	4.3	More Details
CVE-2024-48290	An issue in the Bluetooth Low Energy implementation of Realtek RTL8762E BLE SDK v1.4.0 allows attackers to cause a Denial of Service (DoS) via supplying a crafted ll_terminate_ind packet.	4.3	More Details
CVE-2024-11125	A vulnerability was found in GetSimpleCMS 3.3.16 and classified as problematic. This issue affects some unknown processing of the file /admin/profile.php. The manipulation leads to cross-site request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-10965	A vulnerability classified as problematic was found in emqx neuron up to 2.10.0. Affected by this vulnerability is an unknown functionality of the file /api/v2/schema of the component JSON File Handler. The manipulation leads to information disclosure. The attack can be launched remotely. The patch is named c9ce39747e0372aaa2157b2b56174914a12c06d8. It is recommended to apply a patch to fix this issue.	4.3	More Details
CVE-2024-9926	The Jetpack WordPress plugin does not have proper authorisation in one of its REST endpoint, allowing any authenticated users, such as subscriber to read arbitrary feedbacks data sent via the Jetpack Contact Form	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33660	An exploit is possible where an actor with physical access can manipulate SPI flash without being detected.	4.3	More Details
CVE-2020-11917	An issue was discovered in Siime Eye 14.1.00000001.3.330.0.0.3.14. It uses a default SSID value, which makes it easier for remote attackers to discover the physical locations of many Siime Eye devices, violating the privacy of users who do not wish to disclose their ownership of this type of device. (Various resources such as wigle.net can be use for mapping of SSIDs to physical locations.)	4.3	More Details
CVE-2024-50559	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.2), RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2) (All versions < V8.2), SCALANCE M804PB (6GK5804-0AP00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1AA00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1BA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2) (All versions < V8.2), SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) (All versions < V8.2), SCALANCE M874-2 (6GK5874-2AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 (6GK5874-3AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2) (All versions < V8.2), SCALANCE M876-3 (6GK5876-3AA02-2BA2) (All versions < V8.2), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.2), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.2), SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) (All versions < V8.2), SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) (All versions < V8.2), SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1) (All versions < V8.2), SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1) (All versions < V8.2), SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) (All versions < V8.2), SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1) (All versions < V8.2), SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1) (All versions < V8.2), SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1) (All versions < V8.2), SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) (All versions < V8.2), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.2), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All versions < V8.2), SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2) (All versions < V8.2). Affected devices do not properly validate the filenames of the certificate. This could allow an authenticated remote attacker to append arbitrary values which will lead to compromise of integrity of the system.	4.3	More Details
CVE-2024-11116	Inappropriate implementation in Blink in Google Chrome prior to 131.0.6778.69 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2024-11117	Inappropriate implementation in FileSystem in Google Chrome prior to 131.0.6778.69 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50558	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.2), RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2) (All versions < V8.2), SCALANCE M804PB (6GK5804-0AP00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1AA00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1BA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2) (All versions < V8.2), SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) (All versions < V8.2), SCALANCE M874-2 (6GK5874-2AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 (6GK5874-3AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2) (All versions < V8.2), SCALANCE M876-3 (6GK5876-3AA02-2BA2) (All versions < V8.2), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.2), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.2), SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) (All versions < V8.2), SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) (All versions < V8.2), SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1) (All versions < V8.2), SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1) (All versions < V8.2), SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) (All versions < V8.2), SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1) (All versions < V8.2), SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1) (All versions < V8.2), SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1) (All versions < V8.2), SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) (All versions < V8.2), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.2), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All versions < V8.2), SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2) (All versions < V8.2). Affected devices improperly manage access control for read-only users. This could allow an attacker to cause a temporary denial of service condition.	4.3	More Details
CVE-2024-36509	An exposure of sensitive system information to an unauthorized control sphere vulnerability [CWE-497] in FortiWeb version 7.6.0, version 7.4.3 and below, version 7.2.10 and below, version 7.0.10 and below, version 6.3.23 and below may allow an authenticated attacker to access the encrypted passwords of other administrators via the "Log Access Event" logs page.	4.2	More Details
CVE-2024-51992	Orchid is a @laravel package that allows for rapid application development of back-office applications, admin/user panels, and dashboards. This vulnerability is a method exposure issue (CWE-749: Exposed Dangerous Method or Function) in the Orchid Platform's asynchronous modal functionality, affecting users of Orchid Platform version 8 through 14.42.x. Attackers could exploit this vulnerability to call arbitrary methods within the `Screen` class, leading to potential brute force of database tables, validation checks against user credentials, and disclosure of the server's real IP address. The issue has been patched in the latest release, version 14.43.0, released on November 6, 2024. Users should upgrade to version 14.43.0 or later to address this vulnerability. If upgrading to version 14.43.0 is not immediately possible, users can mitigate the vulnerability by implementing middleware to intercept and validate requests to asynchronous modal endpoints, allowing only approved methods and parameters.	4.1	More Details
CVE-2024-34673	Improper Input Validation in IpcProtocol in Modem prior to SMR Nov-2024 Release 1 allows local attackers to cause Denial-of-Service.	4.1	More Details
CVE-2023-44255	An exposure of sensitive information to an unauthorized actor [CWE-200] in Fortinet FortiManager before 7.4.2, FortiAnalyzer before 7.4.2 and FortiAnalyzer-BigData before 7.2.5 may allow a privileged attacker with administrative read permissions to read event logs of another adom via crafted HTTP or HTTPs requests.	4.1	More Details
CVE-2024-34677	Exposure of sensitive information in System UI prior to SMR Nov-2024 Release 1 allow local attackers to make malicious apps appear as legitimate.	4.0	More Details
CVE-2024-34679	Incorrect default permissions in Crane prior to SMR Nov-2024 Release 1 allows local attackers to access files with phone privilege.	4.0	More Details
CVE-2024-34680	Use of implicit intent for sensitive communication in WlanTest prior to SMR Nov-2024 Release 1 allows local attackers to get sensitive information.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-30142	HCL BigFix Compliance is affected by a missing secure flag on a cookie. If a secure flag is not set, cookies may be stolen by an attacker using XSS, resulting in unauthorized access or session cookies could be transferred over an unencrypted channel.	3.8	More Details
CVE-2024-20528	A vulnerability in the API of Cisco ISE could allow an authenticated, remote attacker to upload files to arbitrary locations on the underlying operating system of an affected device. To exploit this vulnerability, an attacker would need valid Super Admin credentials. This vulnerability is due to insufficient validation of user-supplied parameters in API requests. An attacker could exploit this vulnerability by sending a crafted API request to an affected device. A successful exploit could allow the attacker to upload custom files to arbitrary locations on the underlying operating system, execute arbitrary code, and elevate privileges to root.	3.8	More Details
CVE-2024-10917	In Eclipse OpenJ9 versions up to 0.47, the JNI function GetStringUTFLength may return an incorrect value which has wrapped around. From 0.48 the value is correct but may be truncated to include a smaller number of characters.	3.7	More Details
CVE-2024-11049	A vulnerability classified as problematic has been found in ZKTeco ZKBio Time 9.0.1. Affected is an unknown function of the file /auth_files/photo/ of the component Image File Handler. The manipulation leads to direct request. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2024-43427	A flaw was found in moodle. When creating an export of site administration presets, some sensitive secrets and keys are not being excluded from the export, which could result in them unintentionally being leaked if the presets are shared with a third party.	3.7	More Details
CVE-2024-11026	A vulnerability was found in Intelligent Apps Freenow App 12.10.0 on Android. It has been rated as problematic. Affected by this issue is some unknown functionality of the file ch/qos/logback/core/net/ssl/SSL.java of the component Keystore Handler. The manipulation of the argument DEFAULT_KEYSTORE_PASSWORD with the input changeit leads to use of hard-coded password. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2024-10927	A vulnerability was found in MonoCMS up to 20240528. It has been classified as problematic. Affected is an unknown function of the file /monofiles/account.php of the component Account Information Page. The manipulation of the argument userid leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-11102	A vulnerability was found in SourceCodester Hospital Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /vm/doctor/edit-doc.php. The manipulation of the argument name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	3.5	More Details
CVE-2020-10368	Certain Cypress (and Broadcom) Wireless Combo chips, when a January 2021 firmware update is not present, allow memory read access via a "Spectra" attack.	3.5	More Details
CVE-2024-10928	A vulnerability was found in MonoCMS up to 20240528. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /monofiles/opensaved.php of the component Posts Page. The manipulation of the argument filtcategory/filtstatus leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-51749	Element is a Matrix web client built using the Matrix React SDK. Versions of Element Web and Desktop earlier than 1.11.85 do not check if thumbnails for attachments, stickers and images are coherent. It is possible to add thumbnails to events trigger a file download once clicked. Fixed in element-web 1.11.85.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-11050	A vulnerability was found in AMTT Hotel Broadband Operation System up to 3.0.3.151204 and classified as problematic. This issue affects some unknown processing of the file /language.php. The manipulation of the argument LangID/LangName/LangEName leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-47799	Exposure of sensitive system information to an unauthorized control sphere issue exists in Mesh Wi-Fi router RP562B firmware version v1.0.2 and earlier. If this vulnerability is exploited, a network-adjacent authenticated attacker may obtain information of the other devices connected through the Wi-Fi.	3.5	More Details
CVE-2024-11070	A vulnerability, which was classified as problematic, has been found in Sanluan PublicCMS 5.202406.d. This issue affects some unknown processing of the file /admin/cmsTagType/save of the component Tag Type Handler. The manipulation of the argument name leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-10926	A vulnerability was found in IBPhoenix ibWebAdmin up to 1.0.2 and classified as problematic. This issue affects some unknown processing of the file /toggle_fold_panel.php of the component Tabelas Section. The manipulation of the argument p leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-47587	Cash Operations does not perform necessary authorization check for an authenticated user, resulting in escalation of privileges causing low impact to confidentiality to the application.	3.5	More Details
CVE-2024-11078	A vulnerability has been found in code-projects Job Recruitment 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /register.php. The manipulation of the argument e 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-2024-51993	Combodo iTop is a web based IT Service Management tool. An attacker accessing a backup file or the database can read some passwords for misconfigured Users. This issue has been addressed in version 3.2.0 and all users are advised to upgrade. Users unable to upgrade are advised to encrypt their backups independently of the iTop application. ### Patches Sanitize parameter ### References N°7631 - Password is stored in clear in the database.	3.4	More Details
CVE-2024-11097	A vulnerability has been found in SourceCodester Student Record Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the component Main Menu. The manipulation leads to infinite loop. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used.	3.3	More Details
CVE-2024-48838	Dell SmartFabric OS10 Software, version(s) 10.5.6.x, 10.5.5.x, 10.5.4.x, 10.5.3.x, contain(s) a Files or Directories Accessible to External Parties vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Filesystem access for attacker.	3.3	More Details
CVE-2024-50211	In the Linux kernel, the following vulnerability has been resolved: udf: refactor inode_bmap() to handle error Refactor inode_bmap() to handle error since udf_next_aext() can return error now. On situations like ftruncate, udf_extend_file() can now detect errors and bail out early without resorting to checking for particular offsets and assuming internal behavior of these functions.	3.3	More Details
CVE-2024-36250	Mattermost versions 9.11.x <= 9.11.2, and 9.5.x <= 9.5.10 fail to protect the mfa code against replay attacks, which allows an attacker to reuse the MFA code within ~30 seconds	3.1	More Details
CVE-2024-11126	A vulnerability was found in Digistar AG-30 Plus 2.6b. It has been classified as problematic. Affected is an unknown function of the component Login Page. The manipulation leads to improper restriction of excessive authentication attempts. The complexity of an attack is rather high. The exploitability is told to be difficult. The vendor was contacted early about this disclosure but did not respond in any way.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50560	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.2), RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2) (All versions < V8.2), SCALANCE M804PB (6GK5804-0AP00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1AA00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1BA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2) (All versions < V8.2), SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) (All versions < V8.2), SCALANCE M874-2 (6GK5874-2AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 (6GK5874-3AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2) (All versions < V8.2), SCALANCE M876-3 (6GK5876-3AA02-2BA2) (All versions < V8.2), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.2), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.2), SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) (All versions < V8.2), SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) (All versions < V8.2), SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1) (All versions < V8.2), SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1) (All versions < V8.2), SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) (All versions < V8.2), SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1) (All versions < V8.2), SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1) (All versions < V8.2), SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1) (All versions < V8.2), SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) (All versions < V8.2), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.2), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All versions < V8.2), SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2) (All versions < V8.2). Affected devices truncates usernames longer than 15 characters when accessed via SSH or Telnet. This could allow an attacker to compromise system integrity.	3.1	More Details
CVE-2024-48011	Dell PowerProtect DD, versions prior to 7.7.5.50, contains an Exposure of Sensitive Information to an Unauthorized Actor vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	3.1	More Details
CVE-2024-50341	symfony/security-bundle is a module for the Symphony PHP framework which provides a tight integration of the Security component into the Symfony full-stack framework. The custom `user_checker` defined on a firewall is not called when Login Programmaticaly with the `Security::login` method, leading to unwanted login. As of versions 6.4.10, 7.0.10 and 7.1.3 the `Security::login` method now ensure to call the configured `user_checker`. All users are advised to upgrade. There are no known workarounds for this vulnerability.	3.1	More Details
CVE-2024-50343	symfony/validator is a module for the Symphony PHP framework which provides tools to validate values. It is possible to trick a `Validator` configured with a regular expression using the `$` metacharacters, with an input ending with `\n`. Symfony as of versions 5.4.43, 6.4.11, and 7.1.4 now uses the `D` regex modifier to match the entire input. Users are advised to upgrade. There are no known workarounds for this vulnerability.	3.1	More Details
CVE-2024-50345	symfony/http-foundation is a module for the Symphony PHP framework which defines an object-oriented layer for the HTTP specification. The `Request` class, does not parse URI with special characters the same way browsers do. As a result, an attacker can trick a validator relying on the `Request` class to redirect users to another domain. The `Request::create` methods now assert the URI does not contain invalid characters as defined by https://url.spec.whatwg.org/. This issue has been patched in versions 5.4.46, 6.4.14, and 7.1.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	3.1	More Details
CVE-2024-10920	A vulnerability was found in mariazevedo88 travels-java-api up to 5.0.1 and classified as problematic. Affected by this issue is the function doFilterInternal of the file travels-java-api-master\src\main\java\io\github\mariazevedo88\travelsjavaapi\filters\JwtAuthenticationTokenFilter.java of the component JWT Secret Handler. The manipulation leads to use of hard-coded cryptographic key . The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used.	3.1	More Details
CVE-2024-50342	symfony/http-client is a module for the Symphony PHP framework which provides powerful methods to fetch HTTP resources synchronously or asynchronously. When using the `NoPrivateNetworkHttpClient`, some internal information is still leaking during host resolution, which leads to possible IP/port enumeration. As of versions 5.4.46, 6.4.14, and 7.1.7 the `NoPrivateNetworkHttpClient` now filters blocked IPs earlier to prevent such leaks. All users are advised to upgrade. There are no known workarounds for this vulnerability.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-11138	A vulnerability classified as problematic has been found in DedeCMS 5.7.116. This affects an unknown part of the file /dede/uploads/dede/friendlink_add.php. The manipulation of the argument logoimg leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2.7	More Details
CVE-2024-10672	The Multiple Page Generator Plugin – MPG plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the mpg_upsert_project_source_block() function in all versions up to, and including, 4.0.2. This makes it possible for authenticated attackers, with editor-level access and above, to delete limited files on the server.	2.7	More Details
CVE-2024-42000	Mattermost versions 9.10.x <= 9.10.2, 9.11.x <= 9.11.1, 9.5.x <= 9.5.9 and 10.0.x <= 10.0.0 fail to properly authorize the requests to /api/v4/channels which allows a User or System Manager, with "Read Groups" permission but with no access for channels to retrieve details about private channels that they were not a member of by sending a request to /api/v4/channels.	2.7	More Details
CVE-2024-47190	Northern.tech Hosted Mender before 2024.07.11 allows SSRF.	2.7	More Details
CVE-2024-34675	Improper access control in Dex Mode prior to SMR Nov-2024 Release 1 allows physical attackers to temporarily access to unlocked screen.	2.4	More Details
CVE-2024-11130	A vulnerability was found in ZZCMS up to 2023. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/msg.php. The manipulation of the argument keyword leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2.4	More Details
CVE-2024-34682	Improper authorization in Settings prior to SMR Nov-2024 Release 1 allows physical attackers to access stored WiFi password in Maintenance Mode.	2.4	More Details
CVE-2024-35274	An improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability [CWE-22] in Fortinet FortiAnalyzer versions below 7.4.2, Fortinet FortiManager versions below 7.4.2 and Fortinet FortiAnalyzer-BigData version 7.4.0 and below 7.2.7 allows a privileged attacker with read write administrative privileges to create non-arbitrary files on a chosen directory via crafted CLI requests.	2.3	More Details
CVE-2024-51755	Twig is a template language for PHP. In a sandbox, an attacker can access attributes of Array-like objects as they were not checked by the security policy. They are now checked via the property policy and the `__isset()` method is now called after the security check. This is a BC break. This issue has been patched in versions 3.11.2 and 3.14.1. All users are advised to upgrade. There are no known workarounds for this issue.	2.2	More Details
CVE-2024-51754	Twig is a template language for PHP. In a sandbox, an attacker can call `__toString()` on an object even if the `__toString()` method is not allowed by the security policy when the object is part of an array or an argument list (arguments to a function or a filter for instance). This issue has been patched in versions 3.11.2 and 3.14.1. All users are advised to upgrade. There are no known workarounds for this issue.	2.2	More Details
CVE-2024-51736	Symphony process is a module for the Symphony PHP framework which executes commands in sub-processes. On Windows, when an executable file named `cmd.exe` is located in the current working directory it will be called by the `Process` class when preparing command arguments, leading to possible hijacking. This issue has been addressed in release versions 5.4.46, 6.4.14, and 7.1.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	0.0	More Details
CVE-2024-52000	Combodo iTop is a simple, web based IT Service Management tool. Affected versions are subject to a reflected Cross-site Scripting (XSS) exploit by way of editing a request's payload which can lead to malicious javascript execution. This issue has been addressed in version 3.2.0 via systematic escaping of error messages when rendering on the page. All users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10923	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in OpenText™ ALM Octane Management allows Stored XSS. The vulnerability could result in a remote code execution attack. This issue affects ALM Octane Management: from 16.2.100 through 24.4.	N/A	More Details
CVE-2024-27530	wasm3 139076a contains a Use-After-Free in ForEachModule.	N/A	More Details
CVE-2024-9998	Rejected reason: The vulnerability has no impact, so it has been deprecated.	N/A	More Details
CVE-2024-50228	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-52010	Zoraxy is a general purpose HTTP reverse proxy and forwarding tool. A command injection vulnerability in the Web SSH feature allows an authenticated attacker to execute arbitrary commands as root on the host. Zoraxy has a Web SSH terminal feature that allows authenticated users to connect to SSH servers from their browsers. In HandleCreateProxySession the request to create an SSH session is handled. An attacker can exploit the username variable to escape from the bash command and inject arbitrary commands into sshCommand. This is possible, because, unlike hostname and port, the username is not validated or sanitized.	N/A	More Details
CVE-2024-50220	In the Linux kernel, the following vulnerability has been resolved: fork: do not invoke uffd on fork if error occurs Patch series "fork: do not expose incomplete mm on fork". During fork we may place the virtual memory address space into an inconsistent state before the fork operation is complete. In addition, we may encounter an error during the fork operation that indicates that the virtual memory address space is invalidated. As a result, we should not be exposing it in any way to external machinery that might interact with the mm or VMAs, machinery that is not designed to deal with incomplete state. We specifically update the fork logic to defer khugepaged and ksm to the end of the operation and only to be invoked if no error arose, and disallow uffd from observing fork events should an error have occurred. This patch (of 2): Currently on fork we expose the virtual address space of a process to userland unconditionally if uffd is registered in VMAs, regardless of whether an error arose in the fork. This is performed in dup_userfaultfd_complete() which is invoked unconditionally, and performs two duties - invoking registered handlers for the UFFD_EVENT_FORK event via dup_fctx(), and clearing down userfaultfd_fork_ctx objects established in dup_userfaultfd(). This is problematic, because the virtual address space may not yet be correctly initialised if an error arose. The change in commit d24062914837 ("fork: use __mt_dup() to duplicate maple tree in dup_mmap()") makes this more pertinent as we may be in a state where entries in the maple tree are not yet consistent. We address this by, on fork error, ensuring that we roll back state that we would otherwise expect to clean up through the event being handled by userland and perform the memory freeing duty otherwise performed by dup_userfaultfd_complete(). We do this by implementing a new function, dup_userfaultfd_fail(), which performs the same loop, only decrementing reference counts. Note that we perform mmgrab() on the parent and child mm's, however userfaultfd_ctx_put() will mmdrop() this once the reference count drops to zero, so we will avoid memory leaks correctly here.	N/A	More Details
CVE-2024-50219	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-50218	In the Linux kernel, the following vulnerability has been resolved: ocfs2: pass u64 to ocfs2_truncate_inline maybe overflow Syzbot reported a kernel BUG in ocfs2_truncate_inline. There are two reasons for this: first, the parameter value passed is greater than ocfs2_max_inline_data_with_xattr, second, the start and end parameters of ocfs2_truncate_inline are "unsigned int". So, we need to add a sanity check for byte_start and byte_len right before ocfs2_truncate_inline() in ocfs2_remove_inode_range(), if they are greater than ocfs2_max_inline_data_with_xattr return -EINVAL.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50212	In the Linux kernel, the following vulnerability has been resolved: lib: alloc_tag_module_unload must wait for pending kfree_rcu calls Ben Greear reports following splat: ------------[cut here]------------ net/netfilter/nf_nat_core.c:1114 module nf_nat func:nf_nat_register_fn has 256 allocated at module unload WARNING: CPU: 1 PID: 10421 at lib/alloc_tag.c:168 alloc_tag_module_unload+0x22b/0x3f0 Modules linked in: nf_nat(-) btrfs ufs qnx4 hfsplus hfs minix vfat msdos fat ... Hardware name: Default string Default string/SKYBAY, BIOS 5.12 08/04/2020 RIP: 0010:alloc_tag_module_unload+0x22b/0x3f0 codetag_unload_module+0x19b/0x2a0 ? codetag_load_module+0x80/0x80 nf_nat module exit calls kfree_rcu on those addresses, but the free operation is likely still pending by the time alloc_tag checks for leaks. Wait for outstanding kfree_rcu operations to complete before checking resolves this warning. Reproducer: unshare -n iptables-nft -t nat -A PREROUTING -p tcp grep nf_nat /proc/allocinfo # will list 4 allocations rmmod nft_chain_nat rmmod nf_nat # will WARN. [akpm@linux-foundation.org: add comment]	N/A	More Details
CVE-2024-50216	In the Linux kernel, the following vulnerability has been resolved: xfs: fix finding a last resort AG in xfs_filestream_pick_ag When the main loop in xfs_filestream_pick_ag fails to find a suitable AG it tries to just pick the online AG. But the loop for that uses args->pag as loop iterator while the later code expects pag to be set. Fix this by reusing the max_pag case for this last resort, and also add a check for impossible case of no AG just to make sure that the uninitialized pag doesn't even escape in theory.	N/A	More Details
CVE-2024-50336	matrix-js-sdk is a Matrix messaging protocol Client-Server SDK for JavaScript. matrix-js-sdk before 34.11.0 is vulnerable to client-side path traversal via crafted MXC URIs. A malicious room member can trigger clients based on the matrix-js-sdk to issue arbitrary authenticated GET requests to the client's homeserver. Fixed in matrix-js-sdk 34.11.1.	N/A	More Details
CVE-2024-10526	Rapid7 Velociraptor MSI Installer versions below 0.73.3 suffer from a vulnerability whereby it creates the installation directory with WRITE_DACL permission to the BUILTIN\\Users group. This allows local users who are not administrators to grant themselves the Full Control permission on Velociraptor's files. By modifying Velociraptor's files, local users can subvert the binary and cause the Velociraptor service to execute arbitrary code as the SYSTEM user, or to replace the Velociraptor binary completely. This issue is fixed in version 0.73.3.	N/A	More Details
CVE-2024-10668	There exists an auth bypass in Google Quickshare where an attacker can upload an unknown file type to a victim. The root cause of the vulnerability lies in the fact that when a Payload Transfer frame of type FILE is sent to Quick Share, the file that is contained in this frame is written to disk in the Downloads folder. Quickshare normally deletes unkown files, however an attacker can send two Payload transfer frames of type FILE and the same payload ID. The deletion logic will only delete the first file and not the second. We recommend upgrading past commit 5d8b9156e0c339d82d3dab0849187e8819ad92c0 or Quick Share Windows v1.0.2002.2	N/A	More Details
CVE-2024-40715	A vulnerability in Veeam Backup & Replication Enterprise Manager has been identified, which allows attackers to perform authentication bypass. Attackers must be able to perform Man-in-the-Middle (MITM) attack to exploit this vulnerability.	N/A	More Details
CVE-2024-34015	Sensitive information disclosure during file browsing due to improper symbolic link handling. The following products are affected: Acronis Backup plugin for cPanel & WHM (Linux) before build 818.	N/A	More Details
CVE-2024-47073	DataEase is an open source data visualization analysis tool that helps users quickly analyze data and gain insights into business trends. In affected versions a the lack of signature verification of jwt tokens allows attackers to forge jwts which then allow access to any interface. The vulnerability has been fixed in v2.10.2 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51758	Filament is a collection of full-stack components for accelerated Laravel development. All Filament features that interact with storage use the `default_filesystem_disk` config option. This allows the user to easily swap their storage driver to something production-ready like `s3` when deploying their app, without having to touch multiple configuration options and potentially forgetting about some. The default disk is set to `public` when you first install Filament, since this allows users to quickly get started developing with a functional disk that allows features such as file upload previews locally without the need to set up an S3 disk with temporary URL support. However, some features of Filament such as exports also rely on storage, and the files that are stored contain data that should often not be public. This is not an issue for the many deployed applications, since many use a secure default disk such as S3 in production. However, [CWE-1188](https://cwe.mitre.org/data/definitions/1188.html) suggests that having the `public` disk as the default disk in Filament is a security vulnerability itself. As such, we have implemented a measure to protect users whereby if the `public` disk is set as the default disk, the exports feature will automatically swap it out for the `local` disk, if that exists. Users who set the default disk to `local` or `s3` already are not affected. If a user wants to continue to use the `public` disk for exports, they can by setting the export disk deliberately. This change has been included in the 3.2.123 release and all users who use the `public` disk are advised to upgrade.	N/A	More Details
CVE-2024-11168	The urllib.parse.urlsplit() and urlparse() functions improperly validated bracketed hosts (`[]`), allowing hosts that weren't IPv6 or IPvFuture. This behavior was not conformant to RFC 3986 and potentially enabled SSRF if a URL is processed by more than one URL parser.	N/A	More Details
CVE-2024-34014	Arbitrary file overwrite during recovery due to improper symbolic link handling. The following products are affected: Acronis Backup plugin for cPanel & WHM (Linux) before build 818, Acronis Backup extension for Plesk (Linux) before build 599, Acronis Backup plugin for DirectAdmin (Linux) before build 181.	N/A	More Details
CVE-2024-10345	In Helix Core versions prior to 2024.2, an unauthenticated remote Denial of Service (DoS) via the shutdown function was identified. Reported by Karol Więsek.	N/A	More Details
CVE-2019-20462	An issue was discovered on Alecto IVM-100 2019-11-12 devices. The device comes with a serial interface at the board level. By attaching to this serial interface and rebooting the device, a large amount of information is disclosed. This includes the view password and the password of the Wi-Fi access point that the device used.	N/A	More Details
CVE-2024-10007	A path collision and arbitrary code execution vulnerability was identified in GitHub Enterprise Server that allowed container escape to escalate to root via ghe-firejail path. Exploitation of this vulnerability requires Enterprise Administrator access to the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise prior to 3.15 and was fixed in versions 3.14.3, 3.13.6, 3.12.11, and 3.11.17. This vulnerability was reported via the GitHub Bug Bounty program.	N/A	More Details
CVE-2024-10824	An authorization bypass vulnerability was identified in GitHub Enterprise Server that allowed unauthorized internal users to access sensitive secret scanning alert data intended only for business owners. This issue could be exploited only by organization members with a personal access token (PAT) and required that secret scanning be enabled on user-owned repositories. This vulnerability affected GitHub Enterprise Server versions after 3.13.0 but prior to 3.14.0 and was fixed in version 3.13.2.	N/A	More Details
CVE-2024-10344	In Helix Core versions prior to 2024.2, an unauthenticated remote Denial of Service (DoS) via the refuse function was identified. Reported by Karol Więsek.	N/A	More Details
CVE-2024-36062	The com.callassistant.android (aka AI Call Assistant & Screener) application 1.174 for Android enables any installed application (with no permissions) to place phone calls without user interaction by sending a crafted intent via the com.callassistant.android.ui.call.incall.InCallActivity component.	N/A	More Details
CVE-2024-8810	A GitHub App installed in organizations could upgrade some permissions from read to write access without approval from an organization administrator. An attacker would require an account with administrator access to install a malicious GitHub App. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.14 and was fixed in versions 3.14.1, 3.13.4, 3.12.9, 3.11.15, and 3.10.17. This vulnerability was reported via the GitHub Bug Bounty program.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2315	APTIOV contains a vulnerability in BIOS where may cause Improper Access Control by a local attacker. Successful exploitation of this vulnerability may lead to unexpected SPI flash modifications and BIOS boot kit launches, also impacting the availability.	N/A	More Details
CVE-2024-10314	In Helix Core versions prior to 2024.2, an unauthenticated remote Denial of Service (DoS) via the auto-generation function was identified. Reported by Karol Więsek.	N/A	More Details
CVE-2024-52301	Laravel is a web application framework. When the register_argc_argv php directive is set to on , and users call any URL with a special crafted query string, they are able to change the environment used by the framework when handling the request. The vulnerability fixed in 6.20.45, 7.30.7, 8.83.28, 9.52.17, 10.48.23, and 11.31.0. The framework now ignores argv values for environment detection on non-cli SAPIs.	N/A	More Details
CVE-2024-8074	Improper Privilege Management vulnerability in Nomysoft Informatics Nomysem allows Collect Data as Provided by Users.This issue affects Nomysem: before 13.10.2024.	N/A	More Details
CVE-2024-35425	vmir e8117 was discovered to contain a segmentation violation via the function_prepare_parse function at /src/vmir_function.c.	N/A	More Details
CVE-2024-52004	MediaCMS is an open source video and media CMS, written in Python/Django and React, featuring a REST API. MediaCMS has been prone to vulnerabilities that upon special cases can lead to remote code execution. All versions before v4.1.0 are susceptible, and users are highly recommended to upgrade. The vulnerabilities are related with insufficient input validation while uploading media content. The condition to exploit the vulnerability is that the portal allows users to upload content. This issue has been patched in version 4.1.0. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2024-52286	Stirling-PDF is a locally hosted web application that allows you to perform various operations on PDF files. In affected versions the Merge functionality takes untrusted user input (file name) and uses it directly in the creation of HTML pages allowing any unauthenticated to execute JavaScript code in the context of the user. The issue stems to the code starting at `Line 24` in `src/main/resources/static/js/merge.js`. The file name is directly being input into InnerHTML with no sanitization on the file name, allowing a malicious user to be able to upload files with names containing HTML tags. As HTML tags can include JavaScript code, this can be used to execute JavaScript code in the context of the user. This is a self-injection style attack and relies on a user uploading the malicious file themselves and it impact only them, not other users. A user might be social engineered into running this to launch a phishing attack. Nevertheless, this breaks the expected security restrictions in place by the application. This issue has been addressed in version 0.32.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2024-10694	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-9542. Reason: This candidate is a reservation duplicate of CVE-2024-9542. Notes: All CVE users should reference CVE-2024-9542 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-7516	A vulnerability in Brocade Fabric OS versions before 9.2.2 could allow man-in-the-middle attackers to conduct remote Service Session Hijacking that may arise from the attacker's ability to forge an SSH key while the Brocade Fabric OS Switch is performing various remote operations initiated by a switch admin.	N/A	More Details
CVE-2024-8534	Memory safety vulnerability leading to memory corruption and Denial of Service in NetScaler ADC and Gateway if the appliance must be configured as a Gateway (VPN Vserver) with RDP Feature enabled OR the appliance must be configured as a Gateway (VPN Vserver) and RDP Proxy Server Profile is created and set to Gateway (VPN Vserver) OR the appliance must be configured as a Auth Server (AAA Vserver) with RDP Feature enabled	N/A	More Details
CVE-2024-8535	Authenticated user can access unintended user capabilities in NetScaler ADC and NetScaler Gateway if the appliance must be configured as a Gateway (SSL VPN, ICA Proxy, CVPN, RDP Proxy) with KCDAccount configuration for Kerberos SSO to access backend resources OR the appliance must be configured as an Auth Server (AAA Vserver) with KCDAccount configuration for Kerberos SSO to access backend resources	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10217	XSS Attack in mar.jar, Monitoring Archive Utility (MAR Utility), monitoringconsolecommon.jar in TIBCO Software Inc TIBCO Hawk and TIBCO Operational Intelligence	N/A	More Details
CVE-2024-10218	XSS Attack in mar.jar, Monitoring Archive Utility (MAR Utility), monitoringconsolecommon.jar in TIBCO Software Inc TIBCO Hawk and TIBCO Operational Intelligence	N/A	More Details
CVE-2024-52001	Combodo iTop is a simple, web based IT Service Management tool. In affected versions portal users are able to access forbidden services information. This issue has been addressed in version 3.2.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2024-52002	Combodo iTop is a simple, web based IT Service Management tool. Several url endpoints are subject to a Cross-Site Request Forgery (CSRF) vulnerability. Please refer to the linked GHSA for the complete list. This issue has been addressed in version 3.2.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2024-35422	vmir e8117 was discovered to contain a heap buffer overflow via the wasm_call function at /src/vmir_wasm_parser.c.	N/A	More Details
CVE-2024-9420	A use-after-free in Ivanti Connect Secure before version 22.7R2.3 and 9.1R18.9 and Ivanti Policy Secure before version 22.7R1.2 allows a remote authenticated attacker to achieve remote code execution	N/A	More Details
CVE-2024-23983	Improper handling of canonical URL-encoding may lead to bypass not properly constrained by request rules.	N/A	More Details
CVE-2024-52009	Atlantis is a self-hosted golang application that listens for Terraform pull request events via webhooks. Atlantis logs contains GitHub credentials (tokens `ghs_...`) when they are rotated. This enables an attacker able to read these logs to impersonate Atlantis application and to perform actions on GitHub. When Atlantis is used to administer a GitHub organization, this enables getting administration privileges on the organization. This was reported in #4060 and fixed in #4667 . The fix was included in Atlantis v0.30.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2024-50808	SeaCms 13.1 is vulnerable to code injection in the notification module of the member message notification module in the backend user module, due to unsafe handling of the "notify" variable in admin_notify.php.	N/A	More Details
CVE-2024-50315	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2024. Notes: none.	N/A	More Details
CVE-2024-51757	happy-dom is a JavaScript implementation of a web browser without its graphical user interface. Versions of happy-dom prior to 15.10.2 may execute code on the host via a script tag. This would execute code in the user context of happy-dom. Users are advised to upgrade to version 15.10.2. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2020-10370	Certain Cypress (and Broadcom) Wireless Combo chips such as CYW43455, when a 2021-01-26 Bluetooth firmware update is not present, allow a Bluetooth outage via a "Spectra" attack.	N/A	More Details
CVE-2024-10941	A malicious website could have included an iframe with an malformed URI resulting in a non-exploitable browser crash. This vulnerability affects Firefox < 126.	N/A	More Details
CVE-2024-10315	In Gliffy Online an insecure configuration was discovered in versions before 4.14.0-6. Reported by Alpha Inferno PVT LTD.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40457	The BGP daemon in Extreme Networks ExtremeXOS (aka EXOS) 30.7.1.1 allows an attacker (who is not on a directly connected network) to cause a denial of service (BGP session reset) because of BGP attribute error mishandling (for attribute 21 and 25). NOTE: the vendor disputes this because it is "evaluating support for RFC 7606 as a future feature" and believes that "customers that have chosen to not require or implement RFC 7606 have done so willingly and with knowledge of what is needed to defend against these types of attacks."	N/A	More Details
CVE-2024-38826	Authenticated users can upload specifically crafted files to leak server resources. This behavior can potentially be used to run a denial of service attack against Cloud Controller. The Cloud Foundry project recommends upgrading the following releases: * Upgrade capi release version to 1.194.0 or greater * Upgrade cf-deployment version to v44.1.0 or greater. This includes a patched capi release	N/A	More Details
CVE-2024-50200	In the Linux kernel, the following vulnerability has been resolved: maple_tree: correct tree corruption on spanning store Patch series "maple_tree: correct tree corruption on spanning store", v3. There has been a nasty yet subtle maple tree corruption bug that appears to have been in existence since the inception of the algorithm. This bug seems far more likely to happen since commit f8d112a4e657 ("mm/mmap: avoid zeroing vma tree in mmap_region()"), which is the point at which reports started to be submitted concerning this bug. We were made definitely aware of the bug thanks to the kind efforts of Bert Karwatzki who helped enormously in my being able to track this down and identify the cause of it. The bug arises when an attempt is made to perform a spanning store across two leaf nodes, where the right leaf node is the rightmost child of the shared parent, AND the store completely consumes the right-mode node. This results in mas_wr_spanning_store() mitakenly duplicating the new and existing entries at the maximum pivot within the range, and thus maple tree corruption. The fix patch corrects this by detecting this scenario and disallowing the mistaken duplicate copy. The fix patch commit message goes into great detail as to how this occurs. This series also includes a test which reliably reproduces the issue, and asserts that the fix works correctly. Bert has kindly tested the fix and confirmed it resolved his issues. Also Mikhail Gavrilov kindly reported what appears to be precisely the same bug, which this fix should also resolve. This patch (of 2): There has been a subtle bug present in the maple tree implementation from its inception. This arises from how stores are performed - when a store occurs, it will overwrite overlapping ranges and adjust the tree as necessary to accommodate this. A range may always ultimately span two leaf nodes. In this instance we walk the two leaf nodes, determine which elements are not overwritten to the left and to the right of the start and end of the ranges respectively and then rebalance the tree to contain these entries and the newly inserted one. This kind of store is dubbed a 'spanning store' and is implemented by mas_wr_spanning_store(). In order to reach this stage, mas_store_gfp() invokes mas_wr_preallocate(), mas_wr_store_type() and mas_wr_walk() in turn to walk the tree and update the object (mas) to traverse to the location where the write should be performed, determining its store type. When a spanning store is required, this function returns false stopping at the parent node which contains the target range, and mas_wr_store_type() marks the mas->store_type as wr_spanning_store to denote this fact. When we go to perform the store in mas_wr_spanning_store(), we first determine the elements AFTER the END of the range we wish to store (that is, to the right of the entry to be inserted) - we do this by walking to the NEXT pivot in the tree (i.e. r_mas.last + 1), starting at the node we have just determined contains the range over which we intend to write. We then turn our attention to the entries to the left of the entry we are inserting, whose state is represented by l_mas, and copy these into a 'big node', which is a special node which contains enough slots to contain two leaf node's worth of data. We then copy the entry we wish to store immediately after this - the copy and the insertion of the new entry is performed by mas_store_b_node(). After this we copy the elements to the right of the end of the range which we are inserting, if we have not exceeded the length of the node (i.e. r_mas.offset <= r_mas.end). Herein lies the bug - under very specific circumstances, this logic can break and corrupt the maple tree. Consider the following tree: Height 0 Root Node / \ pivot = 0xffff / \ pivot = ULONG_MAX / ---truncated---	N/A	More Details
CVE-2024-50199	In the Linux kernel, the following vulnerability has been resolved: mm/swapfile: skip HugeTLB pages for unuse_vma I got a bad pud error and lost a 1GB HugeTLB when calling swapoff. The problem can be reproduced by the following steps: 1. Allocate an anonymous 1GB HugeTLB and some other anonymous memory. 2. Swapout the above anonymous memory. 3. run swapoff and we will get a bad pud error in kernel message: mm/pgtable-generic.c:42: bad pud 00000000743d215d(84000001400000e7) We can tell that pud_clear_bad is called by pud_none_or_clear_bad in unuse_pud_range() by ftrace. And therefore the HugeTLB pages will never be freed because we lost it from page table. We can skip HugeTLB pages for unuse_vma to fix it.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8068	Privilege escalation to NetworkService Account access in Citrix Session Recording when an attacker is an authenticated user in the same Windows Active Directory domain as the session recording server domain	N/A	More Details
CVE-2024-51990	jj, or Jujutsu, is a Git-compatible VCS written in rust. In affected versions specially crafted Git repositories can cause `jj` to write files outside the clone. This issue has been addressed in version 0.23.0. Users are advised to upgrade. Users unable to upgrade should avoid cloning repos from unknown sources.	N/A	More Details
CVE-2024-10922	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-51647. Reason: This candidate is a reservation duplicate of CVE-2024-51647. Notes: All CVE users should reference CVE-2024-51647 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-33658	APTIOV contains a vulnerability in BIOS where an attacker may cause an Improper Restriction of Operations within the Bounds of a Memory Buffer by local. Successful exploitation of this vulnerability may lead to privilege escalation and potentially arbitrary code execution, and impact Integrity.	N/A	More Details