SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 11 September 2024

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-6795	In Connex health portal released before8/30/2024, SQL injection vulnerabilities were found that could have allowed an unauthenticated attacker to gain unauthorized access to Connex portal's database. An attacker could have submitted a crafted payload to Connex portal that could have resulted in modification and disclosure of database content and/or perform administrative operations including shutting down the database.	10.0	More Details
CVE-2024-45409	The Ruby SAML library is for implementing the client side of a SAML authorization. Ruby-SAML in <= 12.2 and 1.13.0 <= 1.16.0 does not properly verify the signature of the SAML Response. An unauthenticated attacker with access to any signed saml document (by the IdP) can thus forge a SAML Response/Assertion with arbitrary contents. This would allow the attacker to log in as arbitrary user within the vulnerable system. This vulnerability is fixed in 1.17.0 and 1.12.3.	10.0	More Details
CVE-2024-45032	A vulnerability has been identified in Industrial Edge Management Pro (All versions < V1.9.5), Industrial Edge Management Virtual (All versions < V2.3.1-1). Affected components do not properly validate the device tokens. This could allow an unauthenticated remote attacker to impersonate other devices onboarded to the system.	10.0	More Details
CVE-2024-43102	Concurrent removals of certain anonymous shared memory mappings by using the UMTX_SHM_DESTROY sub-request of UMTX_OP_SHM can lead to decreasing the reference count of the object representing the mapping too many times, causing it to be freed too early. A malicious code exercizing the UMTX_SHM_DESTROY sub-request in parallel can panic the kernel or enable further Use-After-Free attacks, potentially including code execution or Capsicum sandbox escape.	10.0	More Details
CVE-2024-7591	Improper Input Validation vulnerability in Progress LoadMaster allows OS Command Injection.This issue affects: * LoadMaster: 7.2.40.0 and above * ECS: All versions * Multi-Tenancy: 7.1.35.4 and above	10.0	More Details
CVE-2024-45076	IBM webMethods Integration 10.15 could allow an authenticated user to upload and execute arbitrary files which could be executed on the underlying operating system.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8463	File upload restriction bypass vulnerability in PHPGurukul Job Portal 1.0, the exploitation of which could allow an authenticated user to execute an RCE via webshell.	9.9	More Details
CVE-2024-37288	A deserialization issue in Kibana can lead to arbitrary code execution when Kibana attempts to parse a YAML document containing a crafted payload. This issue only affects users that use Elastic Security's built-in AI tools https://www.elastic.co/guide/en/security/current/ai-for-security.html and have configured an Amazon Bedrock connector https://www.elastic.co/guide/en/security/current/assistant-connect-to-bedrock.html .	9.9	More Details
CVE-2024-44902	A deserialization vulnerability in Thinkphp v6.1.3 to v8.0.4 allows attackers to execute arbitrary code.	9.8	More Details
CVE-2024-44849	Qualitor up to 8.24 is vulnerable to Remote Code Execution (RCE) via Arbitrary File Upload in checkAcesso.php.	9.8	More Details
CVE-2024-44721	SeaCMS v13.1 was discovered to a Server-Side Request Forgery (SSRF) via the url parameter at /admin_reslib.php.	9.8	More Details
CVE-2024-7950	The WP Job Portal – A Complete Recruitment System for Company or Job Board website plugin for WordPress is vulnerable to Local File Inclusion, Arbitrary Settings Update, and User Creation in all versions up to, and including, 2.1.6 via several functions called by the 'checkFormRequest' function. This makes it possible for unauthenticated attackers to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included. Attackers can also update arbitrary settings and create user accounts even when registration is disabled, leading to user creation with a default role of Administrator.	9.8	More Details
CVE-2024-44410	D-Link DI-8300 v16.07.26A1 is vulnerable to command injection via the upgrade_filter_asp function.	9.8	More Details
CVE-2024-8584	Orca HCM from LEARNING DIGITAL does not properly restrict access to a specific functionality, allowing unauthenticated remote attacker to exploit this functionality to create an account with administrator privilege and subsequently use it to log in. (The vendor is currently addressing the vulnerability. Once the fix is completed, we will provide information on the affected versions.)	9.8	More Details
CVE-2024-6928	The Opti Marketing WordPress plugin through 2.0.9 does not properly sanitise and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection.	9.8	More Details
CVE-2024-6924	The TrueBooker WordPress plugin before 1.0.3 does not properly sanitise and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection.	9.8	More Details
CVE-2024-40711	A deserialization of untrusted data vulnerability with a malicious payload can allow an unauthenticated remote code execution (RCE).	9.8	More Details
CVE-2024-45771	RapidCMS v1.3.1 was discovered to contain a SQL injection vulnerability via the password parameter at /resource/runlogin.php.	9.8	More Details
CVE-2024-7015	Improper Authentication, Missing Authentication for Critical Function, Improper Authorization vulnerability in Profelis Informatics and Consulting PassBox allows Authentication Abuse.This issue affects PassBox: before v1.2.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6596	An unauthenticated remote attacker can run malicious c# code included in curve files and execute commands in the users context.	9.8	More Details
CVE-2024-44411	D-Link DI-8300 v16.07.26A1 is vulnerable to command injection via the msp_info_htm function.	9.8	More Details
CVE-2024-6342	**UNSUPPORTED WHEN ASSIGNED** A command injection vulnerability in the export-cgi program of Zyxel NAS326 firmware versions through V5.21(AAZF.18)C0 and NAS542 firmware versions through V5.21(ABAG.15)C0 could allow an unauthenticated attacker to execute some operating system (OS) commands by sending a crafted HTTP POST request.	9.8	More Details
CVE-2024-6926	The Viral Signup WordPress plugin through 2.1 does not properly sanitise and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection	9.8	More Details
CVE-2024-33698	A vulnerability has been identified in Opcenter Execution Foundation (All versions), Opcenter Quality (All versions), Opcenter RDL (All versions), SIMATIC Information Server 2022 (All versions), SIMATIC Information Server 2024 (All versions), SIMATIC PCS neo V4.0 (All versions), SIMATIC PCS neo V4.1 (All versions < V4.1 Update 2), SIMATIC PCS neo V5.0 (All versions), SINEC NMS (All versions), Totally Integrated Automation Portal (TIA Portal) V16 (All versions), Totally Integrated Automation Portal (TIA Portal) V17 (All versions < V17 Update 8), Totally Integrated Automation Portal (TIA Portal) V18 (All versions < V18 Update 5), Totally Integrated Automation Portal (TIA Portal) V19 (All versions < V19 Update 3). Affected products contain a heap-based buffer overflow vulnerability in the integrated UMC component. This could allow an unauthenticated remote attacker to execute arbitrary code.	9.8	More Details
CVE-2024-40754	Heap-based Buffer Overflow vulnerability in Samsung Open Source Escargot JavaScript engine allows Overflow Buffers.This issue affects Escargot: 4.0.0.	9.8	More Details
CVE-2023-37226	Loftware Spectrum before 4.6 HF14 has Missing Authentication for a Critical Function.	9.8	More Details
CVE-2023-37227	Loftware Spectrum before 4.6 HF13 Deserializes Untrusted Data.	9.8	More Details
CVE-2023-37231	Loftware Spectrum before 4.6 HF14 uses a Hard-coded Password.	9.8	More Details
CVE-2023-36103	Command Injection vulnerability in goform/SetIPTVCfg interface of Tenda AC15 V15.03.05.20 allows remote attackers to run arbitrary commands via crafted POST request.	9.8	More Details
CVE-2023-37234	Loftware Spectrum through 4.6 has unprotected JMX Registry.	9.8	More Details
CVE-2024-44677	eladmin v2.7 and before is vulnerable to Server-Side Request Forgery (SSRF) which allows an attacker to execute arbitrary code via the DatabaseController.java component.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43491	Microsoft is aware of a vulnerability in Servicing Stack that has rolled back the fixes for some vulnerabilities affecting Optional Components on Windows 10, version 1507 (initial version released July 2015). This means that an attacker could exploit these previously mitigated vulnerabilities on Windows 10, version 1507 (Windows 10 Enterprise 2015 LTSB and Windows 10 IoT Enterprise 2015 LTSB) systems that have installed the Windows security update released on March 12, 2024—KB5035858 (OS Build 10240.20526) or other updates released until August 2024. All later versions of Windows 10 are not impacted by this vulnerability. This servicing stack vulnerability is addressed by installing the September 2024 Servicing stack update (SSU KB5043936) AND the September 2024 Windows security update (KB5043083), in that order. Note: Windows 10, version 1507 reached the end of support (EOS) on May 9, 2017 for devices running the Pro, Home, Enterprise, Education, and Enterprise IoT editions. Only Windows 10 Enterprise 2015 LTSB and Windows 10 IoT Enterprise 2015 LTSB editions are still under support.	9.8	More Details
CVE-2024-44893	An issue in the component /jeecg-boot/jmreport/dict/list of JimuReport v1.7.8 allows attacker to escalate privileges via a crafted GET request.	9.8	More Details
CVE-2024-44839	RapidCMS v1.3.1 was discovered to contain a SQL injection vulnerability via the articleid parameter at /default/article.php.	9.8	More Details
CVE-2024-44838	RapidCMS v1.3.1 was discovered to contain a SQL injection vulnerability via the username parameter at /resource/runlogin.php.	9.8	More Details
CVE-2024-8517	SPIP before 4.3.2, 4.2.16, and 4.1.18 is vulnerable to a command injection issue. A remote and unauthenticated attacker can execute arbitrary operating system commands by sending a crafted multipart file upload HTTP request.	9.8	More Details
CVE-2024-8469	SQL injection vulnerability, by which an attacker could send a specially designed query through id parameter in /jobportal/admin/employee/index.php, and retrieve all the information stored in it.	9.8	More Details
CVE-2024-45507	Server-Side Request Forgery (SSRF), Improper Control of Generation of Code ('Code Injection') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 18.12.16. Users are recommended to upgrade to version 18.12.16, which fixes the issue.	9.8	More Details
CVE-2024-8289	The MultiVendorX – The Ultimate WooCommerce Multivendor Marketplace Solution plugin for WordPress is vulnerable to privilege escalation/de-escalation and account takeover due to an insufficient capability check on the update_item_permissions_check and create_item_permissions_check functions in all versions up to, and including, 4.2.0. This makes it possible for unauthenticated attackers to change the password of any user with the vendor role, create new users with the vendor role, and demote other users like administrators to the vendor role.	9.8	More Details
CVE-2024-44400	A vulnerability was discovered in DI_8400-16.07.26A1, which has been classified as critical. This issue affects the upgrade_filter_asp function in the upgrade_filter.asp file. Manipulation of the path parameter can lead to command injection.	9.8	More Details
CVE-2024-7012	An authentication bypass vulnerability has been identified in Foreman when deployed with External Authentication, due to the puppet-foreman configuration. This issue arises from Apache's mod_proxy not properly unsetting headers because of restrictions on underscores in HTTP headers, allowing authentication through a malformed header. This flaw impacts all active Satellite deployments (6.13, 6.14 and 6.15) and could potentially enable unauthorized users to gain administrative access.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7923	An authentication bypass vulnerability has been identified in Pulpcore when deployed with Gunicorn versions prior to 22.0, due to the puppet-pulpcore configuration. This issue arises from Apache's mod_proxy not properly unsetting headers because of restrictions on underscores in HTTP headers, allowing authentication through a malformed header. This flaw impacts all active Satellite deployments (6.13, 6.14 and 6.15) which are using Pulpcore version 3.0+ and could potentially enable unauthorized users to gain administrative access.	9.8	More Details
CVE-2024-7076	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Semtek Informatics Software Consulting Inc. Semtek Sempos allows Blind SQL Injection.This issue affects Semtek Sempos: through 31072024.	9.8	More Details
CVE-2024-7078	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Semtek Informatics Software Consulting Inc. Semtek Sempos allows SQL Injection.This issue affects Semtek Sempos: through 31072024.	9.8	More Details
CVE-2024-44808	An issue in Vypor Attack API System v.1.0 allows a remote attacker to execute arbitrary code via the user GET parameter.	9.8	More Details
CVE-2024-20439	A vulnerability in Cisco Smart Licensing Utility could allow an unauthenticated, remote attacker to log in to an affected system by using a static administrative credential. This vulnerability is due to an undocumented static user credential for an administrative account. An attacker could exploit this vulnerability by using the static credentials to log in to the affected system. A successful exploit could allow the attacker to log in to the affected system with administrative privileges over the API of the Cisco Smart Licensing Utility application.	9.8	More Details
CVE-2024-8464	SQL injection vulnerability, by which an attacker could send a specially designed query through JOBREGID parameter in /jobportal/admin/applicants/controller.php, and retrieve all the information stored in it.	9.8	More Details
CVE-2024-8465	SQL injection vulnerability, by which an attacker could send a specially designed query through user_id parameter in /jobportal/admin/user/controller.php, and retrieve all the information stored in it.	9.8	More Details
CVE-2024-8467	SQL injection vulnerability, by which an attacker could send a specially designed query through id parameter in /jobportal/admin/category/index.php, and retrieve all the information stored in it.	9.8	More Details
CVE-2024-8468	SQL injection vulnerability, by which an attacker could send a specially designed query through search parameter in /jobportal/index.php, and retrieve all the information stored in it.	9.8	More Details
CVE-2024-8466	SQL injection vulnerability, by which an attacker could send a specially designed query through CATEGORY parameter in /jobportal/admin/category/controller.php, and retrieve all the information stored in it.	9.8	More Details
CVE-2024-8470	SQL injection vulnerability, by which an attacker could send a specially designed query through CATEGORY parameter in /jobportal/admin/vacancy/controller.php, and retrieve all the information stored in it.	9.8	More Details
CVE-2024-45158	An issue was discovered in Mbed TLS 3.6 before 3.6.1. A stack buffer overflow in mbedtls_ecdsa_der_to_raw() and mbedtls_ecdsa_raw_to_der() can occur when the bits parameter is larger than the largest supported curve. In some configurations with PSA disabled, all values of bits are affected. (This never happens in internal library calls, but can affect applications that call these functions directly.)	9.8	More Details
CVE-2024-44402	D-Link DI-8100G 17.12.20A1 is vulnerable to Command Injection via msp_info.htm.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44401	D-Link DI-8100G 17.12.20A1 is vulnerable to Command Injection via sub47A60C function in the upgrade_filter.asp file	9.8	More Details
CVE-2024-7493	The WPCOM Member plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.5.2.1. This is due to the plugin allowing arbitrary data to be passed to wp_insert_user() during registration. This makes it possible for unauthenticated attackers to update their role to that of an administrator during registration.	9.8	More Details
CVE-2024-8292	The WP-Recall – Registration, Profile, Commerce & More plugin for WordPress is vulnerable to privilege escalation/account takeover in all versions up to, and including, 16.26.8. This is due to to plugin not properly verifying a user's identity during new order creation. This makes it possible for unauthenticated attackers to supply any email through the user_email field and update the password for that user during new order creation. This requires the commerce addon to be enabled in order to exploit.	9.8	More Details
CVE-2024-8395	FlyCASS CASS and KCM systems did not correctly filter SQL queries, which made them vulnerable to attack by outside attackers with no authentication.	9.8	More Details
CVE-2024-45159	An issue was discovered in Mbed TLS 3.x before 3.6.1. With TLS 1.3, when a server enables optional authentication of the client, if the client-provided certificate does not have appropriate values in if keyUsage or extKeyUsage extensions, then the return value of mbedtls_ssl_get_verify_result() would incorrectly have the MBEDTLS_X509_BADCERT_KEY_USAGE and MBEDTLS_X509_BADCERT_KEY_USAGE bits clear. As a result, an attacker that had a certificate valid for uses other than TLS client authentication would nonetheless be able to use it for TLS client authentication. Only TLS 1.3 servers were affected, and only with optional authentication (with required authentication, the handshake would be aborted with a fatal alert).	9.8	More Details
CVE-2024-44727	Sourcecodehero Event Management System1.0 is vulnerable to SQL Injection via the parameter 'username' in /event/admin/login.php.	9.8	More Details
CVE-2024-8503	An unauthenticated attacker can leverage a time-based SQL injection vulnerability in VICIdial to enumerate database records. By default, VICIdial stores plaintext credentials within the database.	9.8	More Details
CVE-2024-40643	Joplin is a free, open source note taking and to-do application. Joplin fails to take into account that "<" followed by a non letter character will not be considered html. As such it is possible to do an XSS by putting an "illegal" tag within a tag.	9.6	More Details
CVE-2024-24759	MindsDB is a platform for building artificial intelligence from enterprise data. Prior to version 23.12.4.2, a threat actor can bypass the server-side request forgery protection on the whole website with DNS Rebinding. The vulnerability can also lead to denial of service. Version 23.12.4.2 contains a patch.	9.3	More Details
CVE-2024-42500	HPE has identified a denial of service vulnerability in HPE HP-UX System's Network File System (NFSv4) services.	9.3	More Details
CVE-2024-45053	Fides is an open-source privacy engineering platform. Starting in version 2.19.0 and prior to version 2.44.0, the Email Templating feature uses Jinja2 without proper input sanitization or rendering environment restrictions, allowing for Server-Side Template Injection that grants Remote Code Execution to privileged users. A privileged user refers to an Admin UI user with the default \`Owner\` or \`Contributor\` role, who can escalate their access and execute code on the underlying Fides Webserver container where the Jinja template rendering function is executed. The vulnerability has been patched in Fides version \`2.44.0\`. Users are advised to upgrade to this version or later to secure their systems against this threat. There are no workarounds.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42885	SQL Injection vulnerability in ESAFENET CDG 5.6 and before allows an attacker to execute arbitrary code via the id parameter of the data.jsp page.	9.1	More Details
CVE-2024-35783	A vulnerability has been identified in SIMATIC BATCH V9.1 (All versions), SIMATIC Information Server 2020 (All versions), SIMATIC Information Server 2022 (All versions), SIMATIC PCS 7 V9.1 (All versions < V9.1 SP2 UC06), SIMATIC Process Historian 2020 (All versions), SIMATIC Process Historian 2022 (All versions), SIMATIC WinCC Runtime Professional V18 (All versions < V18 Update 5), SIMATIC WinCC Runtime Professional V19 (All versions < V19 Update 3), SIMATIC WinCC V7.4 (All versions), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 18), SIMATIC WinCC V8.0 (All versions < V8.0 Update 5). The affected products run their DB server with elevated privileges which could allow an authenticated attacker to execute arbitrary OS commands with administrative privileges.	9.1	More Details
CVE-2024-45758	H2O.ai H2O through 3.46.0.4 allows attackers to arbitrarily set the JDBC URL, leading to deserialization attacks, file reads, and command execution. Exploitation can occur when an attacker has access to post to the ImportSQLTable URI with a JSON document containing a connection_url property with any typical JDBC Connection URL attack payload such as one that uses queryInterceptors.	9.1	More Details
CVE-2024-43040	Renwoxing Enterprise Intelligent Management System before v3.0 was discovered to contain a SQL injection vulnerability via the parid parameter at /fx/baseinfo/SearchInfo.	9.1	More Details
CVE-2024-45593	Nix is a package manager for Linux and other Unix systems. A bug in Nix 2.24 prior to 2.24.6 allows a substituter or malicious user to craft a NAR that, when unpacked by Nix, causes Nix to write to arbitrary file system locations to which the Nix process has access. This will be with root permissions when using the Nix daemon. This issue is fixed in Nix 2.24.6.	9.0	More Details
CVE-2024-38220	Azure Stack Hub Elevation of Privilege Vulnerability	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-21897	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later	8.9	More Details
CVE-2024-21898	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later	8.8	More Details
CVE-2024-32763	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later	8.8	More Details
CVE-2024-38225	Microsoft Dynamics 365 Business Central Elevation of Privilege Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44844	DrayTek Vigor3900 v1.5.1.6 was discovered to contain an authenticated command injection vulnerability via the name parameter in the run_command function.	8.8	More Details
CVE-2024-44845	DrayTek Vigor3900 v1.5.1.6 was discovered to contain an authenticated command injection vulnerability via the value parameter in the filter_string function.	8.8	More Details
CVE-2024-45034	Apache Airflow versions before 2.10.1 have a vulnerability that allows DAG authors to add local settings to the DAG folder and get it executed by the scheduler, where the scheduler is not supposed to execute code submitted by the DAG author. Users are advised to upgrade to version 2.10.1 or later, which has fixed the vulnerability.	8.8	More Details
CVE-2024-45498	Example DAG: example_inlet_event_extra.py shipped with Apache Airflow version 2.10.0 has a vulnerability that allows an authenticated attacker with only DAG trigger permission to execute arbitrary commands. If you used that example as the base of your DAGs - please review if you have not copied the dangerous example; see https://github.com/apache/airflow/pull/41873 for more information. We recommend against exposing the example DAGs in your deployment. If you must expose the example DAGs, upgrade Airflow to version 2.10.1 or later.	8.8	More Details
CVE-2024-7112	The Pinpoint Booking System – #1 WordPress Booking Plugin plugin for WordPress is vulnerable to SQL Injection via the 'schedule' parameter in all versions up to, and including, 2.9.9.5.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2024-38018	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-37980	Microsoft SQL Server Elevation of Privilege Vulnerability	8.8	More Details
CVE-2024-37965	Microsoft SQL Server Elevation of Privilege Vulnerability	8.8	More Details
CVE-2024-37341	Microsoft SQL Server Elevation of Privilege Vulnerability	8.8	More Details
CVE-2024-37340	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-37339	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-37338	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-38260	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8104	The The Ultimate WordPress Toolkit – WP Extended plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 3.0.8 via the download_file_ajax function. This makes it possible for authenticated attackers, with subscriber access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	8.8	More Details
CVE-2024-8102	The The Ultimate WordPress Toolkit – WP Extended plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the module_all_toggle_ajax() function in all versions up to, and including, 3.0.8. 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.	8.8	More Details
CVE-2024-43469	Azure CycleCloud Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-8247	The Newsletters plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 4.9.9.2. This is due to the plugin not restricting what user meta can be updated as screen options. This makes it possible for authenticated attackers, with subscriber-level access and above, to escalate their privileges to that of an administrator. Please note that this only affects users with access to edit/update screen options, which means an administrator would need to grant lower privilege users with access to the Sent & Draft Emails page of the plugin in order for this to be exploited.	8.8	More Details
CVE-2024-26186	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-50360	A SQL injection vulnerability has been reported to affect Video Station. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following version: Video Station 5.8.1 (2024/02/26) and later	8.8	More Details
CVE-2024-43455	Windows Remote Desktop Licensing Service Spoofing Vulnerability	8.8	More Details
CVE-2024-2166	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Forcepoint Email Security (Real Time Monitor modules) allows Reflected XSS.This issue affects Email Security: before 8.5.5 HF003.	8.8	More Details
CVE-2024-42416	The ctl_report_supported_opcodes function did not sufficiently validate a field provided by userspace, allowing an arbitrary write to a limited amount of kernel help memory. Malicious software running in a guest VM that exposes virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host.	8.8	More Details
CVE-2024-43110	The ctl_request_sense function could expose up to three bytes of the kernel heap to userspace. Malicious software running in a guest VM that exposes virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45063	The function ctl_write_buffer incorrectly set a flag which resulted in a kernel Use-After-Free when a command finished processing. Malicious software running in a guest VM that exposes virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host.	8.8	More Details
CVE-2024-43461	Windows MSHTML Platform Spoofing Vulnerability	8.8	More Details
CVE-2024-8178	The ctl_write_buffer and ctl_read_buffer functions allocated memory to be returned to userspace, without initializing it. Malicious software running in a guest VM that exposes virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host.	8.8	More Details
CVE-2024-44587	itsourcecode Alton Management System 1.0 is vulnerable to SQL Injection in /noncombo_save.php via the "menu" parameter.	8.8	More Details
CVE-2024-45173	An issue was discovered in za-internet C-MOR Video Surveillance 5.2401. Due to improper privilege management concerning sudo privileges, C-MOR is vulnerable to a privilege escalation attack. The Linux user www-data running the C-MOR web interface can execute some OS commands as root via Sudo without having to enter the root password. These commands, for example, include cp, chown, and chmod, which enable an attacker to modify the system's sudoers file in order to execute all commands with root privileges. Thus, it is possible to escalate the limited privileges of the user www-data to root privileges.	8.8	More Details
CVE-2024-45171	An issue was discovered in za-internet C-MOR Video Surveillance 5.2401. Due to improper user input validation, it is possible to upload dangerous files, for instance PHP code, to the C-MOR system. By analyzing the C-MOR web interface, it was found out that the upload functionality for backup files allows an authenticated user to upload arbitrary files. The only condition is that the filename contains a .cbkf string. Therefore, webshell.cbkf.php is considered a valid file name for the C-MOR web application. Uploaded files are stored within the directory "/srv/www/backups" on the C-MOR system, and can thus be accessed via the URL https://<HOST>/backup/upload_<FILENAME>. Due to broken access control, low-privileged authenticated users can also use this file upload functionality.	8.8	More Details
CVE-2024-45175	An issue was discovered in za-internet C-MOR Video Surveillance 5.2401. Sensitive information is stored in cleartext. It was found out that sensitive information, for example login credentials of cameras, is stored in cleartext. Thus, an attacker with filesystem access, for example exploiting a path traversal attack, has access to the login data of all configured cameras, or the configured FTP server.	8.8	More Details
CVE-2024-45075	IBM webMethods Integration 10.15 could allow an authenticated user to create scheduler tasks that would allow them to escalate their privileges to administrator due to missing authentication.	8.8	More Details
CVE-2024-8480	The Image Optimizer, Resizer and CDN – Sirv plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'sirv_save_prevented_sizes' function in all versions up to, and including, 7.2.7. This makes it possible for authenticated attackers, with Contributor-level access and above, to exploit the 'sirv_upload_file_by_chunks_callback' function, which lacks proper file type validation, allowing attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44739	Sourcecodester Simple Forum Website v1.0 has a SQL injection vulnerability in /php-sqlite-forum/?page=manage_user&id=.	8.8	More Details
CVE-2024-8428	The ForumWP – Forum & Discussion Board Plugin plugin for WordPress is vulnerable to Privilege Escalation via Insecure Direct Object Reference in all versions up to, and including, 2.0.2 via the submit_form_handler due to missing validation on the 'user_id' user controlled key. This makes it possible for authenticated attackers, with subscriber-level access and above, to change the email address of administrative user accounts which can then be leveraged to reset the administrative users password and gain access to their account.	8.8	More Details
CVE-2023-34974	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later	8.8	More Details
CVE-2024-44817	SQL Injection vulnerability in ZZCMS v.2023 and before allows a remote attacker to obtain sensitive information via the id parameter in the adv2.php component.	8.8	More Details
CVE-2024-26191	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-37335	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-44103	DLL hijacking in the management console of Ivanti Workspace Control version 10.18.0.0 and below allows a local authenticated attacker to escalate their privileges.	8.8	More Details
CVE-2024-7770	The Bit File Manager – 100% Free & Open Source File Manager and Code Editor for WordPress plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'upload' function in all versions up to, and including, 6.5.5. This makes it possible for authenticated attackers, with Subscriber-level access and above, and granted upload permissions by an administrator, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2024-43385	A low privileged remote attacker can trigger the execution of arbitrary OS commands as root due to improper neutralization of special elements in the variable PROXY_HTTP_PORT in mGuard devices.	8.8	More Details
CVE-2024-43386	A low privileged remote attacker can trigger the execution of arbitrary OS commands as root due to improper neutralization of special elements in the variable EMAIL_NOTIFICATION.TO in mGuard devices.	8.8	More Details
CVE-2024-43387	A low privileged remote attacker can read and write files as root due to improper neutralization of special elements in the variable EMAIL_RELAY_PASSWORD in mGuard devices.	8.8	More Details
CVE-2024-43388	A low privileged remote attacker with write permissions can reconfigure the SNMP service due to improper input validation.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8268	The Frontend Dashboard plugin for WordPress is vulnerable to unauthorized code execution due to insufficient filtering on callable methods/functions via the ajax_request() function in all versions up to, and including, 2.2.4. This makes it possible for authenticated attackers, with subscriber-level access and above, to call arbitrary functions that can be leverage for privilege escalation by changing user's passwords.	8.8	More Details
CVE-2024-44107	DLL hijacking in the management console of Ivanti Workspace Control version 10.18.0.0 and below allows a local authenticated attacker to escalate their privileges and achieve arbitrary code execution.	8.8	More Details
CVE-2024-7699	An low privileged remote attacker can execute OS commands with root privileges due to improper neutralization of special elements in user data.	8.8	More Details
CVE-2024-41171	A vulnerability has been identified in SINUMERIK 828D V4 (All versions), SINUMERIK 828D V5 (All versions < V5.24), SINUMERIK 840D sl V4 (All versions), SINUMERIK ONE (All versions < V6.24). Affected devices do not properly enforce access restrictions to scripts that are regularly executed by the system with elevated privileges. This could allow an authenticated local attacker to escalate their privileges in the underlying system.	8.8	More Details
CVE-2024-44106	Insufficient server-side controls in the management console of Ivanti Workspace Control version 10.18.0.0 and below allows a local authenticated attacker to escalate their privileges.	8.8	More Details
CVE-2024-44104	An incorrectly implemented authentication scheme that is subjected to a spoofing attack in the management console of Ivanti Workspace Control version 10.18.0.0 and below allows a local authenticated attacker to escalate their privileges.	8.8	More Details
CVE-2024-8504	An attacker with authenticated access to VICIdial as an "agent" can execute arbitrary shell commands as the "root" user. This attack can be chained with CVE-2024-8503 to execute arbitrary shell commands starting from an unauthenticated perspective.	8.8	More Details
CVE-2024-44335	D-Link DI-7003G v19.12.24A1, DI-7003GV2 v24.04.18D1, DI-7100G+V2 v24.04.18D1, DI-7100GV2 v24.04.18D1, DI-7200GV2 v24.04.18E1, DI-7300G+V2 v24.04.18D1, and DI-7400G+V2 v24.04.18D1 are vulnerable to Remote Command Execution (RCE) via version_upgrade.asp.	8.8	More Details
CVE-2024-44334	D-Link DI-7003GV2 v24.04.18D1, DI-7100G+V2 v24.04.18D1, DI-7100GV2 v24.04.18D1, DI-7200GV2 v24.04.18E1, DI-7300G+V2 v24.04.18D1, and DI-7400G+V2 v24.04.18D1 are vulnerable to Remote Command Execution due to insufficient parameter filtering in the CGI handling function of upgrade_filter.asp.	8.8	More Details
CVE-2024-44333	D-Link DI-7003GV2 v24.04.18D1, DI-7100G+V2 v24.04.18D1, DI-7100GV2 v24.04.18D1, DI-7200GV2 v24.04.18E1, DI-7300G+V2 v24.04.18D1, and DI-7400G+V2 v24.04.18D1 are vulnerable to Remote Command Execution. An attacker can achieve arbitrary command execution by sending a carefully crafted malicious string to the CGI function responsible for handling usb_paswd.asp.	8.8	More Details
CVE-2024-38259	Microsoft Management Console Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-8575	A vulnerability was found in TOTOLINK AC1200 T8 4.1.5cu.861_B20230220 and classified as critical. This issue affects the function setWiFiScheduleCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument desc leads to buffer overflow. 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.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8579	A vulnerability classified as critical has been found in TOTOLINK AC1200 T8 4.1.5cu.861_B20230220. This affects the function setWiFiRepeaterCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument password leads to buffer overflow. 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.	8.8	More Details
CVE-2024-8577	A vulnerability was found in TOTOLINK AC1200 T8 and AC1200 T10 4.1.5cu.861_B20230220/4.1.8cu.5207. It has been declared as critical. Affected by this vulnerability is the function setStaticDhcpRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument desc leads to buffer overflow. 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.	8.8	More Details
CVE-2023-37229	Loftware Spectrum before 5.1 allows SSRF.	8.8	More Details
CVE-2024-8578	A vulnerability was found in TOTOLINK AC1200 T8 4.1.5cu.861_B20230220. It has been rated as critical. Affected by this issue is the function setWiFiMeshName of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument device_name leads to buffer overflow. 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.	8.8	More Details
CVE-2023-37230	Loftware Spectrum (testDeviceConnection) before 5.1 allows SSRF.	8.8	More Details
CVE-2023-37233	Loftware Spectrum before 4.6 HF14 allows authenticated XXE attacks.	8.8	More Details
CVE-2024-45044	Bareos is open source software for backup, archiving, and recovery of data for operating systems. When a command ACL is in place and a user executes a command in bconsole using an abbreviation (i.e. "w" for "whoami") the ACL check did not apply to the full form (i.e. "whoami") but to the abbreviated form (i.e. "w"). If the command ACL is configured with negative ACL that should forbid using the "whoami" command, you could still use "w" or "who" as a command successfully. Fixes for the problem are shipped in Bareos versions 23.0.4, 22.1.6 and 21.1.11. If only positive command ACLs are used without any negation, the problem does not occur.	8.8	More Details
CVE-2024-8576	A vulnerability was found in TOTOLINK AC1200 T8 and AC1200 T10 4.1.5cu.861_B20230220/4.1.8cu.5207. It has been classified as critical. Affected is the function setIpPortFilterRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument desc leads to buffer overflow. 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.	8.8	More Details
CVE-2024-8573	A vulnerability, which was classified as critical, was found in TOTOLINK AC1200 T8 and AC1200 T10 4.1.5cu.861_B20230220/4.1.8cu.5207. This affects the function setParentalRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument desc leads to buffer overflow. 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.	8.8	More Details
CVE-2023-51366	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45294	The HL7 FHIR Core Artifacts repository provides the java core object handling code, with utilities (including validator), for the Fast Healthcare Interoperability Resources (FHIR) specification. Prior to version 6.3.23, XSLT transforms performed by various components are vulnerable to XML external entity injections. A processed XML file with a malicious DTD tag 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 issue has been patched in release 6.3.23. No known workarounds are available.	8.6	More Details
CVE-2024-34657	Stack-based out-of-bounds write in Samsung Notes prior to version 4.4.21.62 allows remote attackers to execute arbitrary code.	8.6	More Details
CVE-2024-44087	A vulnerability has been identified in Automation License Manager V5 (All versions), Automation License Manager V6.0 (All versions), Automation License Manager V6.2 (All versions < V6.2 Upd3). Affected applications do not properly validate certain fields in incoming network packets on port 4410/tcp. This could allow an unauthenticated remote attacker to cause an integer overflow and crash of the application. This denial of service condition could prevent legitimate users from using subsequent products that rely on the affected application for license verification.	8.6	More Details
CVE-2024-43479	Microsoft Power Automate Desktop Remote Code Execution Vulnerability	8.5	More Details
CVE-2024-45411	Twig is a template language for PHP. Under some circumstances, the sandbox security checks are not run which allows user-contributed templates to bypass the sandbox restrictions. This vulnerability is fixed in 1.44.8, 2.16.1, and 3.14.0.	8.5	More Details
CVE-2024-45288	A missing null-termination character in the last element of an nvlist array string can lead to writing outside the allocated buffer.	8.4	More Details
CVE-2024-41928	Malicious software running in a guest VM can exploit the buffer overflow to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process.	8.4	More Details
CVE-2024-38194	An authenticated attacker can exploit an improper authorization vulnerability in Azure Web Apps to elevate privileges over a network.	8.4	More Details
CVE-2024-45041	External Secrets Operator is a Kubernetes operator that integrates external secret management systems. The external-secrets has a deployment called default-external-secrets-cert-controller, which is bound with a same-name ClusterRole. This ClusterRole has "get/list" verbs of secrets resources. It also has path/update verb of validatingwebhookconfigurations resources. This can be used to abuse the SA token of the deployment to retrieve or get ALL secrets in the whole cluster, capture and log all data from requests attempting to update Secrets, or make a webhook deny all Pod create and update requests. This vulnerability is fixed in 0.10.2.	8.3	More Details
CVE-2024-32668	An insufficient boundary validation in the USB code could lead to an out-of-bounds write on the heap, with data controlled by the caller. A malicious, privileged software running in a guest VM can exploit the vulnerability to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process.	8.2	More Details
CVE-2024-45592	auditor-bundle, formerly known as DoctrineAuditBundle, integrates auditor library into any Symfony 3.4+ application. Prior to version 5.2.6, there is an unescaped entity property enabling Javascript injection. This is possible because \`%source_label%\` in twig macro is not escaped. Therefore script tags can be inserted and are executed. The vulnerability is fixed in versions 6.0.0 and 5.2.6.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6796	In Baxter Connex health portal released before 8/30/2024, an improper access control vulnerability has been found that could allow an unauthenticated attacker to gain unauthorized access to Connex portal's database and/or modify content.	8.2	More Details
CVE-2024-38216	Azure Stack Hub Elevation of Privilege Vulnerability	8.2	More Details
CVE-2024-44105	Cleartext transmission of sensitive information in the management console of Ivanti Workspace Control version 10.18.0.0 and below allows a local authenticated attacker to obtain OS credentials.	8.2	More Details
CVE-2024-32762	A cross-site scripting (XSS) vulnerability has been reported to affect QuLog Center. If exploited, the vulnerability could allow users to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QuLog Center 1.8.0.872 (2024/06/17) and later QuLog Center 1.7.0.827 (2024/06/17) and later	8.2	More Details
CVE-2024-38240	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	8.1	More Details
CVE-2024-39583	Dell PowerScale InsightIQ, versions 5.0 through 5.1, contains a Use of a Broken or Risky Cryptographic Algorithm vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges.	8.1	More Details
CVE-2024-7627	The Bit File Manager plugin for WordPress is vulnerable to Remote Code Execution in versions 6.0 to 6.5.5 via the 'checkSyntax' function. This is due to writing a temporary file to a publicly accessible directory before performing file validation. This makes it possible for unauthenticated attackers to execute code on the server if an administrator has allowed Guest User read permissions.	8.1	More Details
CVE-2024-38045	Windows TCP/IP Remote Code Execution Vulnerability	8.1	More Details
CVE-2024-8580	A vulnerability classified as critical was found in TOTOLINK AC1200 T8 4.1.5cu.861_B20230220. This vulnerability affects unknown code of the file /etc/shadow.sample. The manipulation leads to use of hard-coded password. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.1	More Details
CVE-2024-43389	A low privileged remote attacker can perform configuration changes of the ospf service through OSPF_INTERFACE.SIMPLE_KEY, OSPF_INTERFACE.DIGEST_KEY environment variables which can lead to a DoS.	8.1	More Details
CVE-2024-43390	A low privileged remote attacker can perform configuration changes of the firewall services, including packet forwarding or NAT through the FW_NAT.IN_IP environment variable which can lead to a DoS.	8.1	More Details
CVE-2024-43391	A low privileged remote attacker can perform configuration changes of the firewall services, including packet filter, packet forwarding, network access control or NAT through the FW_PORTFORWARDING.SRC_IP environment variable which can lead to a DoS.	8.1	More Details
CVE-2024-43392	A low privileged remote attacker can perform configuration changes of the firewall services, including packet filter, packet forwarding, network access control or NAT through the FW_INCOMING.FROM_IP FW_INCOMING.IN_IP FW_OUTGOING.FROM_IP FW_OUTGOING.IN_IP environment variable which can lead to a DoS.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43393	A low privileged remote attacker can perform configuration changes of the firewall services, including packet filter, packet forwarding, network access control or NAT through the FW_INCOMING.FROM_IP FW_INCOMING.IN_IP FW_OUTGOING.FROM_IP FW_OUTGOING.IN_IP FW_RULESETS.FROM_IP FW_RULESETS.IN_IP environment variable which can lead to a DoS.	8.1	More Details
CVE-2024-21416	Windows TCP/IP Remote Code Execution Vulnerability	8.1	More Details
CVE-2024-41716	Cleartext storage of sensitive information vulnerability exists in WindLDR and WindO/I-NV4. If this vulnerability is exploited, an attacker who obtained the product's project file may obtain user credentials of the PLC or Operator Interfaces. As a result, an attacker may be able to manipulate and/or suspend the PLC and Operator Interfaces by accessing or hijacking them.	8.1	More Details
CVE-2024-45174	An issue was discovered in za-internet C-MOR Video Surveillance 5.2401 and 6.00PL01. Due to improper validation of user-supplied data, different functionalities of the C-MOR web interface are vulnerable to SQL injection attacks. This kind of attack allows an authenticated user to execute arbitrary SQL commands in the context of the corresponding MySQL database.	8.1	More Details
CVE-2024-45170	An issue was discovered in za-internet C-MOR Video Surveillance 5.2401. Due to improper or missing access control, low privileged users can use administrative functions of the C-MOR web interface. It was found out that different functions are only available to administrative users. However, access those functions is restricted via the web application user interface and not checked on the server side. Thus, by sending corresponding HTTP requests to the web server of the C-MOR web interface, low privileged users can also use administrative functionality, for instance downloading backup files or changing configuration settings.	8.1	More Details
CVE-2024-43402	Rust is a programming language. The fix for CVE-2024-24576, where `std::process::Command` incorrectly escaped arguments when invoking batch files on Windows, was incomplete. Prior to Rust version 1.81.0, it was possible to bypass the fix when the batch file name had trailing whitespace or periods (which are ignored and stripped by Windows). To determine whether to apply the `cmd.exe` escaping rules, the original fix for the vulnerability checked whether the command name ended with `.bat` or `.cmd`. At the time that seemed enough, as we refuse to invoke batch scripts with no file extension. Windows removes trailing whitespace and periods when parsing file paths. For example, `.bat. .` is interpreted by Windows as `.bat`, but the original fix didn't check for that. Affected users who are using Rust 1.77.2 or greater can remove the trailing whitespace (ASCII 0x20) and trailing periods (ASCII 0x2E) from the batch file name to bypass the incomplete fix and enable the mitigations. Users are affected if their code or one of their dependencies invoke a batch script on Windows with trailing whitespace or trailing periods in the name, and pass untrusted arguments to it. Rust 1.81.0 will update the standard library to apply the CVE-2024-24576 mitigations to all batch files invocations, regardless of the trailing chars in the file name.	8.1	More Details
CVE-2024-44667	Shenzhen Haichangxing Technology Co., Ltd HCX H822 4G LTE Router M7628NNxISPxUIv2_v1.0.1557.15.35_P0 is vulnerable to Incorrect Access Control. Unauthenticated factory mode reset and command injection leads to information exposure and root shell access.	8.0	More Details
CVE-2024-44859	Tenda FH1201 v1.2.0.14 has a stack buffer overflow vulnerability in `formWrlExtraGet`.	8.0	More Details
CVE-2024-39585	Dell SmartFabric OS10 Software, version(s) 10.5.5.4 through 10.5.5.10 and 10.5.6.x, contain(s) an Use of Hard-coded Password vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Client-side request forgery and Information disclosure.	7.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44951	In the Linux kernel, the following vulnerability has been resolved: serial: sc16is7xx: fix TX fifo corruption Sometimes, when a packet is received on channel A at almost the same time as a packet is about to be transmitted on channel B, we observe with a logic analyzer that the received packet on channel A is transmitted on channel B. In other words, the Tx buffer data on channel B is corrupted with data from channel A. The problem appeared since commit 4409df5866b7 ("serial: sc16is7xx: change EFR lock to operate on each channels"), which changed the EFR locking to operate on each channel instead of chip-wise. This commit has introduced a regression, because the EFR lock is used not only to protect the EFR registers access, but also, in a very obscure and undocumented way, to protect access to the data buffer, which is shared by the Tx and Rx handlers, but also by each channel of the IC. Fix this regression first by switching to kfifo_out_linear_ptr() in sc16is7xx_handle_tx() to eliminate the need for a shared Rx/Tx buffer. Secondly, replace the chip-wise Rx buffer with a separate Rx buffer for each channel.	7.8	More Details
CVE-2024-44986	In the Linux kernel, the following vulnerability has been resolved: ipv6: fix possible UAF in ip6_finish_output2() If skb_expand_head() returns NULL, skb has been freed and associated dst/idev could also have been freed. We need to hold rcu_read_lock() to make sure the dst and associated idev are alive.	7.8	More Details
CVE-2024-38238	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38241	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38242	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-43463	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-38243	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-44985	In the Linux kernel, the following vulnerability has been resolved: ipv6: prevent possible UAF in ip6_xmit() If skb_expand_head() returns NULL, skb has been freed and the associated dst/idev could also have been freed. We must use rcu_read_lock() to prevent a possible UAF.	7.8	More Details
CVE-2024-38244	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44987	In the Linux kernel, the following vulnerability has been resolved: ipv6: prevent UAF in ip6_send_skb() syzbot reported an UAF in ip6_send_skb() [1] After ip6_local_out() has returned, we no longer can safely dereference rt, unless we hold rcu_read_lock(). A similar issue has been fixed in commit a688caa34beb ("ipv6: take rcu lock in rawv6_send_hdrinc()") Another potential issue in ip6_finish_output2() is handled in a separate patch. [1] BUG: KASAN: slab-use-after-free in ip6_send_skb+0x18d/0x230 net/ipv6/ip6_output.c:1964 Read of size 8 at addr ffff88806dde4858 by task syz.1.380/6530 CPU: 1 UID: 0 PID: 6530 Comm: syz.1.380 Not tainted 6.11.0-rc3-syzkaller-00306-gdf6cbc62cc9b #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/06/2024 Call Trace: <TASK> __dump_stack lib/dump_stack.c:93 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:119 print_address_description mm/kasan/report.c:377 [inline] print_report+0x169/0x550 mm/kasan/report.c:488 kasan_report+0x143/0x180 mm/kasan/report.c:601 ip6_send_skb+0x18d/0x230 net/ipv6/ip6_output.c:1964 rawv6_push_pending_frames+0x75c/0x9e0 net/ipv6/raw.c:588 rawv6_sendmsg+0x19c7/0x23c0 net/ipv6/raw.c:926 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x1a6/0x270 net/socket.c:745 sock_write_iter+0x2dd/0x400 net/socket.c:1160 do_iter_readv_writev+0x60a/0x890 vfs_writev+0x37c/0xbb0 fs/read_write.c:971 do_writev+0x1b1/0x350 fs/read_write.c:1018 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: 0033:0x7f936bf79e79 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 a8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f936cd7f038 EFLAGS: 00000246 ORIG_RAX: 0000000000000014 RAX: ffffffffffffffda RBX: 00007f936c115f80 RCX: 00007f936bf79e79 RDX: 0000000000000001 RSI: 0000000020000040 RDI: 0000000000000004 RBP: 00007f936bfe7916 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 0000000000000000 R14: 00007f936c115f80 R15: 00007fff2860a7a8 </TASK> Allocated by task 6530: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 unpoison_slab_object mm/kasan/common.c:312 [inline] __kasan_slab_alloc+0x66/0x80 mm/kasan/common.c:338 kasan_slab_alloc include/linux/kasan.h:201 [inline] slab_post_alloc_hook mm/slub.c:3988 [inline] slab_alloc_node mm/slub.c:4037 [inline] kmem_cache_alloc_noprof+0x135/0x2a0 mm/slub.c:4044 dst_alloc+0x12b/0x190 net/core/dst.c:89 ip6_blackhole_route+0x59/0x340 net/ipv6/route.c:2670 make_blackhole net/xfrm/xfrm_policy.c:3120 [inline] xfrm_lookup_route+0xd1/0x1c0 net/xfrm/xfrm_policy.c:3313 ip6_dst_lookup_flow+0x13e/0x180 net/ipv6/ip6_output.c:1257 rawv6_sendmsg+0x1283/0x23c0 net/ipv6/raw.c:898 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x1a6/0x270 net/socket.c:745 ____sys_sendmsg+0x525/0x7d0 net/socket.c:2597 ___sys_sendmsg net/socket.c:2651 [inline] __sys_sendmsg+0x2b0/0x3a0 net/socket.c:2680 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 Freed by task 45: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 kasan_save_free_info+0x40/0x50 mm/kasan/generic.c:579 poison_slab_object+0xe0/0x150 mm/kasan/common.c:240 __kasan_slab_free+0x37/0x60 mm/kasan/common.c:256 kasan_slab_free include/linux/kasan.h:184 [inline] slab_free_hook mm/slub.c:2252 [inline] slab_free mm/slub.c:4473 [inline] kmem_cache_free+0x145/0x350 mm/slub.c:4548 dst_destroy+0x2ac/0x460 net/core/dst.c:124 rcu_do_batch kernel/rcu/tree.c:2569 [inline] rcu_core+0xafd/0x1830 kernel/rcu/tree. ---truncated---	7.8	More Details
CVE-2024-44977	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Validate TA binary size Add TA binary size validation to avoid OOB write. (cherry picked from commit c0a04e3570d72aaf090962156ad085e37c62e442)	7.8	More Details
CVE-2024-38245	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38247	Windows Graphics Component Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38249	Windows Graphics Component Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38250	Windows Graphics Component Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38252	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38253	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-44997	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: mtk_wed: fix use-after-free panic in mtk_wed_setup_tc_block_cb() When there are multiple ap interfaces on one band and with WED on, turning the interface down will cause a kernel panic on MT798X. Previously, cb_priv was freed in mtk_wed_setup_tc_block() without marking NULL,and mtk_wed_setup_tc_block_cb() didn't check the value, too. Assign NULL after free cb_priv in mtk_wed_setup_tc_block() and check NULL in mtk_wed_setup_tc_block_cb(). ---------- Unable to handle kernel paging request at virtual address 0072460bca32b4f5 Call trace: mtk_wed_setup_tc_block_cb+0x4/0x38 0xffffffc0794084bc tcf_block_playback_offloads+0x70/0x1e8 tcf_block_unbind+0x6c/0xc8 ... ---------	7.8	More Details
CVE-2024-44998	In the Linux kernel, the following vulnerability has been resolved: atm: idt77252: prevent use after free in dequeue_rx() We can't dereference "skb" after calling vcc->push() because the skb is released.	7.8	More Details
CVE-2024-44978	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Free job before xe_exec_queue_put Free job depends on job->vm being valid, the last xe_exec_queue_put can destroy the VM. Prevent UAF by freeing job before xe_exec_queue_put. (cherry picked from commit 32a42c93b74c8ca6d0915ea3eba21bceff53042f)	7.8	More Details
CVE-2024-43465	Microsoft Excel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38237	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-44964	In the Linux kernel, the following vulnerability has been resolved: idpf: fix memory leaks and crashes while performing a soft reset The second tagged commit introduced a UAF, as it removed restoring q_vector->vport pointers after reinitializating the structures. This is due to that all queue allocation functions are performed here with the new temporary vport structure and those functions rewrite the backpointers to the vport. Then, this new struct is freed and the pointers start leading to nowhere. But generally speaking, the current logic is very fragile. It claims to be more reliable when the system is low on memory, but in fact, it consumes two times more memory as at the moment of running this function, there are two vports allocated with their queues and vectors. Moreover, it claims to prevent the driver from running into "bad state", but in fact, any error during the rebuild leaves the old vport in the partially allocated state. Finally, if the interface is down when the function is called, it always allocates a new queue set, but when the user decides to enable the interface later on, vport_open() allocates them once again, IOW there's a clear memory leak here. Just don't allocate a new queue set when performing a reset, that solves crashes and memory leaks. Readd the old queue number and reopen the interface on rollback - that solves limbo states when the device is left disabled and/or without HW queues enabled.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8191	SQL injection in the management console of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to achieve remote code execution.	7.8	More Details
CVE-2024-8012	An authentication bypass weakness in the message broker service of Ivanti Workspace Control version 10.18.0.0 and below allows a local authenticated attacker to escalate their privileges.	7.8	More Details
CVE-2024-8258	Improper Control of Generation of Code ('Code Injection') in Electron Fuses in Logitech Options Plus version 1.60.496306 on macOS allows attackers to execute arbitrary code via insecure Electron Fuses configuration.	7.8	More Details
CVE-2024-41170	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0015), Tecnomatix Plant Simulation V2404 (All versions < V2404.0004). The affected applications contain a stack based overflow vulnerability while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-43492	Microsoft AutoUpdate (MAU) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-31960	An issue was discovered in Samsung Mobile Processor Exynos 1480, Exynos 2400. The xclipse amdgpu driver has a reference count bug. This can lead to a use after free.	7.8	More Details
CVE-2024-30073	Windows Security Zone Mapping Security Feature Bypass Vulnerability	7.8	More Details
CVE-2024-44949	In the Linux kernel, the following vulnerability has been resolved: parisc: fix a possible DMA corruption ARCH_DMA_MINALIGN was defined as 16 - this is too small - it may be possible that two unrelated 16-byte allocations share a cache line. If one of these allocations is written using DMA and the other is written using cached write, the value that was written with DMA may be corrupted. This commit changes ARCH_DMA_MINALIGN to be 128 on PA20 and 32 on PA1.1 - that's the largest possible cache line size. As different parisc microarchitectures have different cache line size, we define arch_slab_minalign(), cache_line_size() and dma_get_cache_alignment() so that the kernel may tune slab cache parameters dynamically, based on the detected cache line size.	7.8	More Details
CVE-2024-38014	Windows Installer Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38046	PowerShell Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-7834	A local privilege escalation is caused by Overwolf loading and executing certain dynamic link library files from a user-writeable folder in SYSTEM context on launch. This allows an attacker with unprivileged access to the system to run arbitrary code with SYSTEM privileges by placing a malicious .dll file in the respective location.	7.8	More Details
CVE-2024-44967	In the Linux kernel, the following vulnerability has been resolved: drm/mgag200: Bind I2C lifetime to DRM device Managed cleanup with devm_add_action_or_reset() will release the I2C adapter when the underlying Linux device goes away. But the connector still refers to it, so this cleanup leaves behind a stale pointer in struct drm_connector.ddc. Bind the lifetime of the I2C adapter to the connector's lifetime by using DRM's managed release. When the DRM device goes away (after the Linux device) DRM will first clean up the connector and then clean up the I2C adapter.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38642	An improper certificate validation vulnerability has been reported to affect QuMagie. If exploited, the vulnerability could allow local network users to compromise the security of the system via unspecified vectors. We have already fixed the vulnerability in the following version: QuMagie 2.3.1 and later	7.8	More Details
CVE-2024-38641	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later	7.8	More Details
CVE-2023-39298	A missing authorization vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow local authenticated users to access data or perform actions that they should not be allowed to perform via unspecified vectors. QuTScloud, is not affected. We have already fixed the vulnerability in the following versions: QTS 5.2.0.2737 build 20240417 and later QuTS hero h5.2.0.2782 build 20240601 and later	7.8	More Details
CVE-2024-44974	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: avoid possible UaF when selecting endp select_local_address() and select_signal_address() both select an endpoint entry from the list inside an RCU protected section, but return a reference to it, to be read later on. If the entry is dereferenced after the RCU unlock, reading info could cause a Use-after-Free. A simple solution is to copy the required info while inside the RCU protected section to avoid any risk of UaF later. The address ID might need to be modified later to handle the ID0 case later, so a copy seems OK to deal with.	7.8	More Details
CVE-2024-43457	Windows Setup and Deployment Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-30584	A vulnerability has been discovered in Node.js version 20, specifically within the experimental permission model. This flaw relates to improper handling of path traversal bypass when verifying file permissions. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.	7.7	More Details
CVE-2024-45392	SuiteCRM is an open-source customer relationship management (CRM) system. Prior to version 7.14.5 and 8.6.2, insufficient access control checks allow a threat actor to delete records via the API. Versions 7.14.5 and 8.6.2 contain a patch for the issue.	7.7	More Details
CVE-2024-43458	Windows Networking Information Disclosure Vulnerability	7.7	More Details
CVE-2024-43476	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	7.6	More Details
CVE-2024-43474	Microsoft SQL Server Information Disclosure Vulnerability	7.6	More Details
CVE-2024-42427	Dell ThinOS versions 2402 and 2405, contains an Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability. An unauthenticated attacker with physical access could potentially exploit this vulnerability, leading to Elevation of privileges.	7.6	More Details
CVE-2024-38263	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8509	A vulnerability was found in Forklift Controller. There is no verification against the authorization header except to ensure it uses bearer authentication. Without an Authorization header and some form of a Bearer token, a 401 error occurs. The presence of a token value provides a 200 response with the requested information.	7.5	More Details
CVE-2024-8232	SpiderControl SCADA Web Server has a vulnerability that could allow an attacker to upload specially crafted malicious files without authentication.	7.5	More Details
CVE-2023-6841	A denial of service vulnerability was found in keycloak where the amount of attributes per object is not limited,an attacker by sending repeated HTTP requests could cause a resource exhaustion when the application send back rows with long attribute values.	7.5	More Details
CVE-2024-45195	Direct Request ('Forced Browsing') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 18.12.16. Users are recommended to upgrade to version 18.12.16, which fixes the issue.	7.5	More Details
CVE-2023-30587	A vulnerability in Node.js version 20 allows for bypassing restrictions set by the --experimental-permission flag using the built-in inspector module (node:inspector). By exploiting the Worker class's ability to create an "internal worker" with the kIsInternal Symbol, attackers can modify the isInternal value when an inspector is attached within the Worker constructor before initializing a new WorkerImpl. This vulnerability exclusively affects Node.js users employing the permission model mechanism. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.	7.5	More Details
CVE-2023-30583	fs.openAsBlob() can bypass the experimental permission model when using the file system read restriction with the `--allow-fs-read` flag in Node.js 20. This flaw arises from a missing check in the `fs.openAsBlob()` API. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.	7.5	More Details
CVE-2024-45296	path-to-regexp turns path strings into a regular expressions. In certain cases, path-to-regexp will output a regular expression that can be exploited to cause poor performance. Because JavaScript is single threaded and regex matching runs on the main thread, poor performance will block the event loop and lead to a DoS. The bad regular expression is generated any time you have two parameters within a single segment, separated by something that is not a period (.). For users of 0.1, upgrade to 0.1.10. All other users should upgrade to 8.0.0.	7.5	More Details
CVE-2024-40681	IBM MQ 9.1 LTS, 9.2 LTS, 9.3 LTS, 9.3 CD, 9.4 LTS, and 9.4 CD could allow an authenticated user in a specifically defined role, to bypass security restrictions and execute actions against the queue manager.	7.5	More Details
CVE-2024-8391	In Eclipse Vert.x version 4.3.0 to 4.5.9, the gRPC server does not limit the maximum length of message payload (Maven GAV: io.vertx:vertx-grpc-server and io.vertx:vertx-grpc-client). This is fixed in the 4.5.10 version. Note this does not affect the Vert.x gRPC server based grpc-java and Netty libraries (Maven GAV: io.vertx:vertx-grpc)	7.5	More Details
CVE-2024-38119	Windows Network Address Translation (NAT) Remote Code Execution Vulnerability	7.5	More Details
CVE-2024-44720	SeaCMS v13.1 was discovered to an arbitrary file read vulnerability via the component admin_safe.php.	7.5	More Details
CVE-2024-34158	Calling Parse on a "// +build" build tag line with deeply nested expressions can cause a panic due to stack exhaustion.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34156	Calling Decoder.Decode on a message which contains deeply nested structures can cause a panic due to stack exhaustion. This is a follow-up to CVE-2022-30635.	7.5	More Details
CVE-2024-39921	Observable timing discrepancy issue exists in IPCOM EX2 Series V01L02NF0001 to V01L06NF0401, V01L20NF0001 to V01L20NF0401, V02L20NF0001 to V02L21NF0301, and IPCOM VE2 Series V01L04NF0001 to V01L06NF0112. If this vulnerability is exploited, some of the encrypted communication may be decrypted by an attacker who can obtain the contents of the communication.	7.5	More Details
CVE-2024-7652	An error in the ECMA-262 specification relating to Async Generators could have resulted in a type confusion, potentially leading to memory corruption and an exploitable crash. This vulnerability affects Firefox < 128, Firefox ESR < 115.13, Thunderbird < 115.13, and Thunderbird < 128.	7.5	More Details
CVE-2024-45506	HAProxy 2.9.x before 2.9.10, 3.0.x before 3.0.4, and 3.1.x through 3.1-dev6 allows a remote denial of service for HTTP/2 zero-copy forwarding (h2_send loop) under a certain set of conditions, as exploited in the wild in 2024.	7.5	More Details
CVE-2024-7884	When a canister method is called via ic_cdk::call* , a new Future CallFuture is created and can be awaited by the caller to get the execution result. Internally, the state of the Future is tracked and stored in a struct called CallFutureState. A bug in the polling implementation of the CallFuture allows multiple references to be held for this internal state and not all references were dropped before the Future is resolved. Since we have unaccounted references held, a copy of the internal state ended up being persisted in the canister's heap and thus causing a memory leak. Impact Canisters built in Rust with ic_cdk and ic_cdk_timers are affected. If these canisters call a canister method, use timers or heartbeat, they will likely leak a small amount of memory on every such operation. In the worst case, this could lead to heap memory exhaustion triggered by an attacker. Motoko based canisters are not affected by the bug. PatchesThe patch has been backported to all minor versions between >= 0.8.0, <= 0.15.0. The patched versions available are 0.8.2, 0.9.3, 0.10.1, 0.11.6, 0.12.2, 0.13.5, 0.14.1, 0.15.1 and their previous versions have been yanked. WorkaroundsThere are no known workarounds at the moment. Developers are recommended to upgrade their canister as soon as possible to the latest available patched version of ic_cdk to avoid running out of Wasm heap memory. Upgrading the canisters (without updating `ic_cdk`) also frees the leaked memory but it's only a temporary solution.	7.5	More Details
CVE-2024-43467	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	7.5	More Details
CVE-2024-8418	A flaw was found in Aardvark-dns, which is vulnerable to a Denial of Service attack due to the serial processing of TCP DNS queries. An attacker can exploit this flaw by keeping a TCP connection open indefinitely, causing the server to become unresponsive and resulting in other DNS queries timing out. This issue prevents legitimate users from accessing DNS services, thereby disrupting normal operations and causing service downtime.	7.5	More Details
CVE-2024-45590	body-parser is Node.js body parsing middleware. body-parser <1.20.3 is vulnerable to denial of service when url encoding is enabled. A malicious actor using a specially crafted payload could flood the server with a large number of requests, resulting in denial of service. This issue is patched in 1.20.3.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43647	A vulnerability has been identified in SIMATIC S7-200 SMART CPU CR40 (6ES7288-1CR40-0AA0) (All versions), SIMATIC S7-200 SMART CPU CR60 (6ES7288-1CR60-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR20 (6ES7288-1SR20-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR20 (6ES7288-1SR20-0AA1) (All versions), SIMATIC S7-200 SMART CPU SR30 (6ES7288-1SR30-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR30 (6ES7288-1SR30-0AA1) (All versions), SIMATIC S7-200 SMART CPU SR40 (6ES7288-1SR40-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR40 (6ES7288-1SR40-0AA1) (All versions), SIMATIC S7-200 SMART CPU SR60 (6ES7288-1SR60-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR60 (6ES7288-1SR60-0AA1) (All versions), SIMATIC S7-200 SMART CPU ST20 (6ES7288-1ST20-0AA0) (All versions), SIMATIC S7-200 SMART CPU ST20 (6ES7288-1ST20-0AA1) (All versions), SIMATIC S7-200 SMART CPU ST30 (6ES7288-1ST30-0AA0) (All versions), SIMATIC S7-200 SMART CPU ST30 (6ES7288-1ST30-0AA1) (All versions), SIMATIC S7-200 SMART CPU ST40 (6ES7288-1ST40-0AA0) (All versions), SIMATIC S7-200 SMART CPU ST40 (6ES7288-1ST40-0AA1) (All versions), SIMATIC S7-200 SMART CPU ST60 (6ES7288-1ST60-0AA0) (All versions), SIMATIC S7-200 SMART CPU ST60 (6ES7288-1ST60-0AA1) (All versions). Affected devices do not properly handle TCP packets with an incorrect structure. This could allow an unauthenticated remote attacker to cause a denial of service condition. To restore normal operations, the network cable of the device needs to be unplugged and re-plugged.	7.5	More Details
CVE-2024-44408	D-Link DIR-823G v1.0.2B05_20181207 is vulnerable to Information Disclosure. The device allows unauthorized configuration file downloads, and the downloaded configuration files contain plaintext user passwords.	7.5	More Details
CVE-2024-23185	Very large headers can cause resource exhaustion when parsing message. The message-parser normally reads reasonably sized chunks of the message. However, when it feeds them to message-header-parser, it starts building up "full_value" buffer out of the smaller chunks. The full_value buffer has no size limit, so large headers can cause large memory usage. It doesn't matter whether it's a single long header line, or a single header split into multiple lines. This bug exists in all Dovecot versions. Incoming mails typically have some size limits set by MTA, so even largest possible header size may still fit into Dovecot's vsz_limit. So attackers probably can't DoS a victim user this way. A user could APPEND larger mails though, allowing them to DoS themselves (although maybe cause some memory issues for the backend in general). One can implement restrictions on headers on MTA component preceding Dovecot. No publicly available exploits are known.	7.5	More Details
CVE-2024-44375	D-Link DI-8100 v16.07.26A1 has a stack overflow vulnerability in the dbsrv_asp function.	7.5	More Details
CVE-2024-38486	Dell SmartFabric OS10 Software, version(s) 10.5.5.4 through 10.5.5.10 and 10.5.6.x , contain(s) an Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	7.5	More Details
CVE-2024-37728	Arbitrary File Read vulnerability in Xi'an Daxi Information Technology Co., Ltd OfficeWeb365 v.7.18.23.0 and v8.6.1.0 allows a remote attacker to obtain sensitive information via the "Pic/Indexes" interface	7.5	More Details
CVE-2024-38236	DHCP Server Service Denial of Service Vulnerability	7.5	More Details
CVE-2024-44867	phpok v3.0 was discovered to contain an arbitrary file read vulnerability via the component /autoload/file.php.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45401	stripe-cli is a command-line tool for the payment processor Stripe. A vulnerability exists in stripe-cli starting in version 1.11.1 and prior to version 1.21.3 where a plugin package containing a manifest with a malformed plugin shortname installed using the --archive-url or --archive-path flags can overwrite arbitrary files. The update in version 1.21.3 addresses the path traversal vulnerability by removing the ability to install plugins from an archive URL or path. There has been no evidence of exploitation of this vulnerability.	7.5	More Details
CVE-2024-38257	Microsoft AllJoyn API Information Disclosure Vulnerability	7.5	More Details
CVE-2024-1744	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Ariva Computer Accord ORS allows Retrieve Embedded Sensitive Data.This issue affects Accord ORS: before 7.3.2.1.	7.5	More Details
CVE-2024-34659	Exposure of sensitive information in GroupSharing prior to version 13.6.13.3 allows remote attackers can force the victim to join the group.	7.5	More Details
CVE-2024-45300	alf.io is an open source ticket reservation system for conferences, trade shows, workshops, and meetups. Prior to version 2.0-M5, a race condition allows the user to bypass the limit on the number of promo codes and use the discount coupon multiple times. In "alf.io", an event organizer can apply price discounts by using promo codes to your events. The organizer can limit the number of promo codes that will be used for this, but the time-gap between checking the number of codes and restricting the use of the codes allows a threat actor to bypass the promo code limit. Version 2.0-M5 fixes this issue.	7.5	More Details
CVE-2024-6445	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in DataFlowX Technology DataDiodeX allows Path Traversal.This issue affects DataDiodeX: from v3.0.0 before v3.1.7.	7.5	More Details
CVE-2024-45692	Webmin before 2.202 and Virtualmin before 7.20.2 allow a network traffic loop via spoofed UDP packets on port 10000.	7.5	More Details
CVE-2024-38233	Windows Networking Denial of Service Vulnerability	7.5	More Details
CVE-2024-45287	A malicious value of size in a structure of packed libnv can cause an integer overflow, leading to the allocation of a smaller buffer than required for the parsed data.	7.5	More Details
CVE-2024-38232	Windows Networking Denial of Service Vulnerability	7.5	More Details
CVE-2023-37232	Loftware Spectrum through 4.6 exposes Sensitive Information (Logs) to an Unauthorized Actor.	7.5	More Details
CVE-2024-20440	A vulnerability in Cisco Smart Licensing Utility could allow an unauthenticated, remote attacker to access sensitive information. This vulnerability is due to excessive verbosity in a debug log file. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain log files that contain sensitive data, including credentials that can be used to access the API.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6572	Improper host key checking in active check 'Check SFTP Service' and special agent 'VNX quotas and filesystem' in Checkmk before Checkmk 2.3.0p15, 2.2.0p33, 2.1.0p48 and 2.0.0 (EOL) allows man-in-the-middle attackers to intercept traffic	7.4	More Details
CVE-2024-45596	Directus is a real-time API and App dashboard for managing SQL database content. An unauthenticated user can access credentials of last authenticated user via OpenID or OAuth2 where the authentication URL did not include redirect query string. This happens because on that endpoint for both OpenId and Oauth2 Directus is using the respond middleware, which by default will try to cache GET requests that met some conditions. Although, those conditions do not include this scenario, when an unauthenticated request returns user credentials. This vulnerability is fixed in 10.13.3 and 11.1.0.	7.4	More Details
CVE-2023-46809	Node.js versions which bundle an unpatched version of OpenSSL or run against a dynamically linked version of OpenSSL which are unpatched are vulnerable to the Marvin Attack - https://people.redhat.com/~hkario/marvin/, if PCKS #1 v1.5 padding is allowed when performing RSA descryption using a private key.	7.4	More Details
CVE-2023-47563	An OS command injection vulnerability has been reported to affect Video Station. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following version: Video Station 5.8.2 and later	7.4	More Details
CVE-2024-43405	Nuclei is a vulnerability scanner powered by YAML based templates. Starting in version 3.0.0 and prior to version 3.3.2, a vulnerability in Nuclei's template signature verification system could allow an attacker to bypass the signature check and possibly execute malicious code via custom code template. The vulnerability is present in the template signature verification process, specifically in the `signer` package. The vulnerability stems from a discrepancy between how the signature verification process and the YAML parser handle newline characters, combined with the way multiple signatures are processed. This allows an attacker to inject malicious content into a template while maintaining a valid signature for the benign part of the template. CLI users are affected if they execute custom code templates from unverified sources. This includes templates authored by third parties or obtained from unverified repositories. SDK Users are affected if they are developers integrating Nuclei into their platforms, particularly if they permit the execution of custom code templates by end-users. The vulnerability is addressed in Nuclei v3.3.2. Users are strongly recommended to update to this version to mitigate the security risk. As an interim measure, users should refrain from using custom templates if unable to upgrade immediately. Only trusted, verified templates should be executed. Those who are unable to upgrade Nuclei should disable running custom code templates as a workaround.	7.4	More Details
CVE-2024-8478	The The Affiliate Super Assistent plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 1.5.3. This is due to the software allowing users to supply arbitrary shortcodes in comments when the 'Parse comments' option is enabled. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	7.3	More Details
CVE-2024-43470	Azure Network Watcher VM Agent Elevation of Privilege Vulnerability	7.3	More Details
CVE-2024-8569	A vulnerability has been found in code-projects Hospital Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file user-login.php. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-43495	Windows libarchive Remote Code Execution Vulnerability	7.3	More Details
CVE-2024-38226	Microsoft Publisher Security Feature Bypass Vulnerability	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39581	Dell PowerScale InsightIQ, versions 5.0 through 5.1, contains a File or Directories Accessible to External Parties vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability to read, modify, and delete arbitrary files.	7.3	More Details
CVE-2024-43475	Microsoft Windows Admin Center Information Disclosure Vulnerability	7.3	More Details
CVE-2024-8565	A vulnerability was found in SourceCodesters Clinics Patient Management System 2.0. It has been rated as critical. This issue affects some unknown processing of the file /print_diseases.php. The manipulation of the argument disease/from/to 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-2024-8567	A vulnerability, which was classified as critical, has been found in itsourcecode Payroll Management System 1.0. This issue affects some unknown processing of the file /ajax.php?action=delete_deductions. 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-2024-34656	Path traversal in Samsung Notes prior to version 4.4.21.62 allows local attackers to execute arbitrary code.	7.3	More Details
CVE-2024-33508	An improper neutralization of special elements used in a command ('Command Injection') vulnerability [CWE-77] in Fortinet FortiClientEMS 7.2.0 through 7.2.4, 7.0.0 through 7.0.12 may allow an unauthenticated attacker to execute limited and temporary operations on the underlying database via crafted requests.	7.3	More Details
CVE-2024-34660	Heap-based out-of-bounds write in Samsung Notes prior to version 4.4.21.62 allows local attackers to execute arbitrary code.	7.3	More Details
CVE-2024-44871	An arbitrary file upload vulnerability in the component /admin/index.php of moziloCMS v3.0 allows attackers to execute arbitrary code via uploading a crafted file.	7.2	More Details
CVE-2024-7349	The LifterLMS – WP LMS for eLearning, Online Courses, & Quizzes plugin for WordPress is vulnerable to blind SQL Injection via the 'order' parameter in all versions up to, and including, 7.7.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with 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.	7.2	More Details
CVE-2024-44725	AutoCMS v5.4 was discovered to contain a SQL injection vulnerability via the sidebar parameter at /admin/robot.php.	7.2	More Details
CVE-2024-38228	Microsoft SharePoint Server Remote Code Execution Vulnerability	7.2	More Details
CVE-2024-8190	An OS command injection vulnerability in Ivanti Cloud Services Appliance versions 4.6 Patch 518 and before allows a remote authenticated attacker to obtain remote code execution. The attacker must have admin level privileges to exploit this vulnerability.	7.2	More Details
CVE-2023-39300	An OS command injection vulnerability has been reported to affect legacy QTS. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 4.3.6.2805 build 20240619 and later QTS 4.3.4.2814 build 20240618 and later QTS 4.3.3.2784 build 20240619 and later QTS 4.2.6 build 20240618 and later	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38227	Microsoft SharePoint Server Remote Code Execution Vulnerability	7.2	More Details
CVE-2024-1596	The Ninja Forms - File Uploads plugin for WordPress is vulnerable to Stored Cross-Site Scripting via an uploaded file (e.g. RTX file) in all versions up to, and including, 3.3.16 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2024-44724	AutoCMS v5.4 was discovered to contain a PHP code injection vulnerability via the txtsite_url parameter at /admin/site_add.php. This vulnerability allows attackers to execute arbitrary PHP code via injecting a crafted value.	7.2	More Details
CVE-2024-38239	Windows Kerberos Elevation of Privilege Vulnerability	7.2	More Details
CVE-2024-43464	Microsoft SharePoint Server Remote Code Execution Vulnerability	7.2	More Details
CVE-2024-37337	Microsoft SQL Server Native Scoring Information Disclosure Vulnerability	7.1	More Details
CVE-2024-45178	An issue was discovered in za-internet C-MOR Video Surveillance 5.2401. Due to improper user input validation, it is possible to download arbitrary files from the C-MOR system via a path traversal attack. It was found out that different functionalities are vulnerable to path traversal attacks, due to insufficient user input validation. For instance, the download functionality for backups provided by the script download-bkf.pml is vulnerable to a path traversal attack via the parameter bkf. This enables an authenticated user to download arbitrary files as Linux user www-data from the C-MOR system. Another path traversal attack is in the script show-movies.pml, which can be exploited via the parameter cam.	7.1	More Details
CVE-2024-44983	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: validate vlan header Ensure there is sufficient room to access the protocol field of the VLAN header, validate it once before the flowtable lookup. === BUG: KMSAN: uninit-value in nf_flow_offload_inet_hook+0x45a/0x5f0 net/netfilter/nf_flow_table_inet.c:32 nf_flow_offload_inet_hook+0x45a/0x5f0 net/netfilter/nf_flow_table_inet.c:32 nf_hook_entry_hookfn include/linux/netfilter.h:154 [inline] nf_hook_slow+0xf4/0x400 net/netfilter/core.c:626 nf_hook_ingress include/linux/netfilter_netdev.h:34 [inline] nf_ingress net/core/dev.c:5440 [inline]	7.1	More Details
CVE-2024-43454	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	7.1	More Details
CVE-2024-38188	Azure Network Watcher VM Agent Elevation of Privilege Vulnerability	7.1	More Details
CVE-2024-7341	A session fixation issue was discovered in the SAML adapters provided by Keycloak. The session ID and JSESSIONID cookie are not changed at login time, even when the turnOffChangeSessionIdOnLogin option is configured. This flaw allows an attacker who hijacks the current session before authentication to trigger session fixation.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45050	Ringer server is the server code for the Ringer messaging app. Prior to version 1.3.1, there is an issue with the messages loading route where Ringer Server does not check to ensure that the user loading the conversation is actually a member of that conversation. This allows any user with a Lif Account to load any conversation between two users without permission. This issue had been patched in version 1.3.1. There is no action required for users. Lif Platforms will update their servers with the patch.	7.1	More Details
CVE-2024-37342	Microsoft SQL Server Native Scoring Information Disclosure Vulnerability	7.1	More Details
CVE-2024-37966	Microsoft SQL Server Native Scoring Information Disclosure Vulnerability	7.1	More Details
CVE-2024-44999	In the Linux kernel, the following vulnerability has been resolved: gtp: pull network headers in gtp_dev_xmit() syzbot/KMSAN reported use of uninit-value in get_dev_xmit() [1] We must make sure the IPv4 or Ipv6 header is pulled in skb->head before accessing fields in them. Use pskb_inet_may_pull() to fix this issue. [1] BUG: KMSAN: uninit-value in ipv6_pdp_find drivers/net/gtp.c:220 [inline] BUG: KMSAN: uninit-value in gtp_build_skb_ip6 drivers/net/gtp.c:1229 [inline] BUG: KMSAN: uninit-value in gtp_dev_xmit+0x1424/0x2540 drivers/net/gtp.c:1281 ipv6_pdp_find drivers/net/gtp.c:220 [inline] gtp_build_skb_ip6 drivers/net/gtp.c:1229 [inline] gtp_dev_xmit+0x1424/0x2540 drivers/net/gtp.c:1281 __netdev_start_xmit include/linux/netdevice.h:4913 [inline] netdev_start_xmit include/linux/netdevice.h:4922 [inline] xmit_one net/core/dev.c:3580 [inline] dev_hard_start_xmit+0x247/0xa20 net/core/dev.c:3596 __dev_queue_xmit+0x358c/0x5610 net/core/dev.c:4423 dev_queue_xmit include/linux/netdevice.h:3105 [inline] packet_xmit+0x9c/0x6c0 net/packet/af_packet.c:276 packet_snd net/packet/af_packet.c:3145 [inline] packet_sendmsg+0x90e3/0xa3a0 net/packet/af_packet.c:3177 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 __sys_sendto+0x685/0x830 net/socket.c:2204 __do_sys_sendto net/socket.c:2216 [inline] __se_sys_sendto net/socket.c:2212 [inline] __x64_sys_sendto+0x125/0x1d0 net/socket.c:2212 x64_sys_call+0x3799/0x3c10 arch/x86/include/generated/asm/syscalls_64.h:45 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:3994 [inline] slab_alloc_node mm/slub.c:4037 [inline] kmem_cache_alloc_node_noprof+0x6bf/0xb80 mm/slub.c:4080 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:583 __alloc_skb+0x363/0x7b0 net/core/skbuff.c:674 alloc_skb include/linux/skbuff.h:1320 [inline] alloc_skb_with_frags+0xc8/0xbf0 net/core/skbuff.c:6526 sock_alloc_send_pskb+0xa81/0xbf0 net/core/sock.c:2815 packet_alloc_skb net/packet/af_packet.c:2994 [inline] packet_snd net/packet/af_packet.c:3088 [inline] packet_sendmsg+0x749c/0xa3a0 net/packet/af_packet.c:3177 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 __sys_sendto+0x685/0x830 net/socket.c:2204 __do_sys_sendto net/socket.c:2216 [inline] __se_sys_sendto net/socket.c:2212 [inline] __x64_sys_sendto+0x125/0x1d0 net/socket.c:2212 x64_sys_call+0x3799/0x3c10 arch/x86/include/generated/asm/syscalls_64.h:45 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f CPU: 0 UID: 0 PID: 7115 Comm: syz.1.515 Not tainted 6.11.0-rc1-syzkaller-00043-g94ede2a3e913 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/27/2024	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44993	In the Linux kernel, the following vulnerability has been resolved: drm/v3d: Fix out-of-bounds read in `v3d_csd_job_run()` When enabling UBSAN on Raspberry Pi 5, we get the following warning: [387.894977] UBSAN: array-index-out-of-bounds in drivers/gpu/drm/v3d/v3d_sched.c:320:3 [387.903868] index 7 is out of range for type '__u32 [7]' [387.909692] CPU: 0 PID: 1207 Comm: kworker/u16:2 Tainted: G WC 6.10.3-v8-16k-numa #151 [387.919166] Hardware name: Raspberry Pi 5 Model B Rev 1.0 (DT) [387.925961] Workqueue: v3d_csd drm_sched_run_job_work [gpu_sched] [387.932525] Call trace: [387.935296] dump_backtrace+0x170/0x1b8 [387.939403] show_stack+0x20/0x38 [387.942907] dump_stack_lvl+0x90/0xd0 [387.946785] dump_stack+0x18/0x28 [387.950301] __ubsan_handle_out_of_bounds+0x98/0xd0 [387.955383] v3d_csd_job_run+0x3a8/0x438 [v3d] [387.960707] drm_sched_run_job_work+0x520/0x6d0 [gpu_sched] [387.966862] process_one_work+0x62c/0xb48 [387.971296] worker_thread+0x468/0x5b0 [387.975317] kthread+0x1c4/0x1e0 [387.978818] ret_from_fork+0x10/0x20 [387.983014] ---[end trace]--- This happens because the UAPI provides only seven configuration registers and we are reading the eighth position of this u32 array. Therefore, fix the out-of-bounds read in `v3d_csd_job_run()` by accessing only seven positions on the '__u32 [7]' array. The eighth register exists indeed on V3D 7.1, but it isn't currently used. That being so, let's guarantee that it remains unused and add a note that it could be set in a future patch.	7.1	More Details
CVE-2024-38246	Win32k Elevation of Privilege Vulnerability	7.0	More Details
CVE-2024-38248	Windows Storage Elevation of Privilege Vulnerability	7.0	More Details
CVE-2024-45098	IBM Aspera Faspex 5.0.0 through 5.0.9 could allow a user to bypass intended access restrictions and conduct resource modification.	6.8	More Details
CVE-2024-31489	AAn improper certificate validation vulnerability [CWE-295] in FortiClientWindows 7.2.0 through 7.2.2, 7.0.0 through 7.0.11, FortiClientLinux 7.2.0, 7.0.0 through 7.0.11 and FortiClientMac 7.0.0 through 7.0.11, 7.2.0 through 7.2.4 may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the FortiGate and the FortiClient during the ZTNA tunnel creation	6.8	More Details
CVE-2024-6979	Amin Aliakbari, member of the AXIS OS Bug Bounty Program, has found a broken access control which would lead to less-privileged operator- and/or viewer accounts having more privileges than designed. The risk of exploitation is very low as it requires complex steps to execute, including knowing of account passwords and social engineering attacks in tricking the administrator to perform specific configurations on operator- and/or viewer-privileged accounts. Axis has released patched AXIS OS a version for the highlighted flaw. Please refer to the Axis security advisory for more information and solution.	6.8	More Details
CVE-2024-44383	WAYOS FBM-291W v19.09.11 is vulnerable to Command Execution via msp_info_htm.	6.8	More Details
CVE-2024-45172	An issue was discovered in za-internet C-MOR Video Surveillance 5.2401 and 6.00PL01. Due to missing protection mechanisms, the C-MOR web interface is vulnerable to cross-site request forgery (CSRF) attacks. The C-MOR web interface offers no protection against cross-site request forgery (CSRF) attacks.	6.8	More Details
CVE-2024-42642	Micron Crucial MX500 Series Solid State Drives M3CR046 is vulnerable to Buffer Overflow, which can be triggered by sending specially crafted ATA packets from the host to the drive controller.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39574	Dell PowerScale InsightIQ, version 5.1, contain an Improper Privilege Management vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Denial of service.	6.7	More Details
CVE-2024-39580	Dell PowerScale InsightIQ, versions 5.0 through 5.1, contains an Improper Access Control vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	6.7	More Details
CVE-2022-27592	An unquoted search path or element vulnerability has been reported to affect QVR Smart Client. If exploited, the vulnerability could allow local authenticated administrators to execute unauthorized code or commands via unspecified vectors. We have already fixed the vulnerability in the following version: Windows 10 SP1, Windows 11, Mac OS, and Mac M1: QVR Smart Client 2.4.0.0570 and later	6.7	More Details
CVE-2024-27387	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_rx_range_done_ind(), there is no input validation check on rtt_id coming from userspace, which can lead to a heap overwrite.	6.7	More Details
CVE-2024-27383	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_get_scan_extra_ies(), there is no input validation check on default_ies coming from userspace, which can lead to a heap overwrite.	6.7	More Details
CVE-2024-34638	Improper handling of exceptional conditions in ThemeCenter prior to SMR Sep-2024 Release 1 allows local attackers to delete non-preloaded applications.	6.7	More Details
CVE-2024-8441	An uncontrolled search path in the agent of Ivanti EPM before 2022 SU6, or the 2024 September update allows a local authenticated attacker with admin privileges to escalate their privileges to SYSTEM.	6.7	More Details
CVE-2024-21903	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later	6.6	More Details
CVE-2023-34979	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2790 build 20240606 and later	6.6	More Details
CVE-2024-34646	Improper access control in DualDarManagerProxy prior to SMR Sep-2024 Release 1 allows local attackers to cause local permanent denial of service.	6.6	More Details
CVE-2024-7620	The Customizer Export/Import plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the '_import' function in all versions up to, and including, 0.9.7. This makes it possible for authenticated attackers, with Administrator-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible. NOTE: This vulnerability is only exploitable when used in conjunction with a race condition as the uploaded file is deleted shortly after it is created.	6.6	More Details
CVE-2024-43487	Windows Mark of the Web Security Feature Bypass Vulnerability	6.5	More Details
CVE-2024-6173	51l3nc3, member of the AXIS OS Bug Bounty Program, has found that a Guard Tour VAPIX API parameter allowed the use of arbitrary values allowing for an attacker to block access to the guard tour configuration page in the web interface of the Axis device. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5956	This vulnerability allows unauthenticated remote attackers to bypass authentication and gain partial data access to the vulnerable Trellix IPS Manager with garbage data in response mostly	6.5	More Details
CVE-2024-45299	alf.io is an open source ticket reservation system for conferences, trade shows, workshops, and meetups. Prior to version 2.0-M5, the preloaded data as json is not escaped correctly, the administrator / event admin could break their own install by inserting non correctly escaped text. The Content-Security-Policy directive blocks any potential script execution. The administrator or event administrator can override the texts for customization purpose. The texts are not properly escaped. Version 2.0-M5 fixes this issue.	6.5	More Details
CVE-2024-45074	IBM webMethods Integration 10.15 could allow an authenticated user to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system.	6.5	More Details
CVE-2024-42495	Credentials to access device configuration were transmitted using an unencrypted protocol. These credentials would allow read-only access to network configuration information and terminal configuration data.	6.5	More Details
CVE-2024-37990	A vulnerability has been identified in SIMATIC Reader RF610R CMIIT (6GT2811-6BC10-2AA0) (All versions < V4.2), SIMATIC Reader RF610R ETSI (6GT2811-6BC10-0AA0) (All versions < V4.2), SIMATIC Reader RF610R FCC (6GT2811-6BC10-1AA0) (All versions < V4.2), SIMATIC Reader RF615R CMIIT (6GT2811-6CC10-2AA0) (All versions < V4.2), SIMATIC Reader RF615R ETSI (6GT2811-6CC10-0AA0) (All versions < V4.2), SIMATIC Reader RF615R FCC (6GT2811-6CC10-1AA0) (All versions < V4.2), SIMATIC Reader RF650R ARIB (6GT2811-6AB20-4AA0) (All versions < V4.2), SIMATIC Reader RF650R CMIIT (6GT2811-6AB20-2AA0) (All versions < V4.2), SIMATIC Reader RF650R ETSI (6GT2811-6AB20-0AA0) (All versions < V4.2), SIMATIC Reader RF650R FCC (6GT2811-6AB20-1AA0) (All versions < V4.2), SIMATIC Reader RF680R ARIB (6GT2811-6AA10-4AA0) (All versions < V4.2), SIMATIC Reader RF680R CMIIT (6GT2811-6AA10-2AA0) (All versions < V4.2), SIMATIC Reader RF680R ETSI (6GT2811-6AA10-0AA0) (All versions < V4.2), SIMATIC Reader RF680R FCC (6GT2811-6AA10-1AA0) (All versions < V4.2), SIMATIC Reader RF685R ARIB (6GT2811-6CA10-4AA0) (All versions < V4.2), SIMATIC Reader RF685R CMIIT (6GT2811-6CA10-2AA0) (All versions < V4.2), SIMATIC Reader RF685R ETSI (6GT2811-6CA10-0AA0) (All versions < V4.2), SIMATIC Reader RF685R FCC (6GT2811-6CA10-1AA0) (All versions < V4.2), SIMATIC RF1140R (6GT2831-6CB00) (All versions < V1.1), SIMATIC RF1170R (6GT2831-6BB00) (All versions < V1.1), SIMATIC RF166C (6GT2002-0EE20) (All versions < V2.2), SIMATIC RF185C (6GT2002-0JE10) (All versions < V2.2), SIMATIC RF186C (6GT2002-0JE20) (All versions < V2.2), SIMATIC RF186CI (6GT2002-0JE50) (All versions < V2.2), SIMATIC RF188C (6GT2002-0JE40) (All versions < V2.2), SIMATIC RF188CI (6GT2002-0JE60) (All versions < V2.2), SIMATIC RF360R (6GT2801-5BA30) (All versions < V2.2). The affected applications contain configuration files which can be modified. An attacker with privilege access can modify these files and enable features that are not released for this device.	6.5	More Details
CVE-2024-8394	When aborting the verification of an OTR chat session, an attacker could have caused a use-after-free bug leading to a potentially exploitable crash. This vulnerability affects Thunderbird < 128.2.	6.5	More Details
CVE-2024-45286	Due to lack of proper authorization checks when calling user, a function module in obsolete Tobin interface in SAP Production and Revenue Accounting allows unauthorized access that could lead to disclosure of highly sensitive data. There is no impact on integrity or availability.	6.5	More Details
CVE-2024-7870	The PixelYourSite – Your smart PIXEL (TAG) & API Manager and the PixelYourSite PRO plugins for WordPress are vulnerable to Sensitive Information Exposure in all versions up to, and including, 9.7.1 and 10.4.2, respectively, through publicly exposed log files. This makes it possible for unauthenticated attackers to view potentially sensitive information contained in the exposed log files, and to delete log files.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6332	The Booking for Appointments and Events Calendar – Amelia Premium and Lite plugins for WordPress are vulnerable to unauthorized access of data due to a missing capability check on the 'ameliaButtonCommand' function in all versions up to, and including, Premium 7.7 and Lite 1.2.3. This makes it possible for unauthenticated attackers to access employee calendar details, including Google Calendar OAuth tokens in the premium version.	6.5	More Details
CVE-2024-38258	Windows Remote Desktop Licensing Service Information Disclosure Vulnerability	6.5	More Details
CVE-2024-45407	Sunshine is a self-hosted game stream host for Moonlight. Clients that experience a MITM attack during the pairing process may inadvertantly allow access to an unintended client rather than failing authentication due to a PIN validation error. The pairing attempt fails due to the incorrect PIN, but the certificate from the forged pairing attempt is incorrectly persisted prior to the completion of the pairing request. This allows access to the certificate belonging to the attacker.	6.5	More Details
CVE-2024-8585	Orca HCM from LEARNING DIGITA does not properly restrict a specific parameter of the file download functionality, allowing a remote attacker with regular privileges to download arbitrary system files.	6.5	More Details
CVE-2024-6509	Marinus Pfund, member of the AXIS OS Bug Bounty Program, has found the VAPIX API alwaysmulti.cgi was vulnerable for file globbing which could lead to resource exhaustion of the Axis device. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution.	6.5	More Details
CVE-2024-45504	Cross-site request forgery (CSRF) vulnerability in multiple Alps System Integration products and the OEM products allow a remote unauthenticated attacker to hijack the authentication of the user and to perform unintended operations if the user views a malicious page while logged in.	6.5	More Details
CVE-2024-38234	Windows Networking Denial of Service Vulnerability	6.5	More Details
CVE-2024-8601	This vulnerability exists in TechExcel Back Office Software versions prior to 1.0.0 due to improper access controls on certain API endpoints. An authenticated remote attacker could exploit this vulnerability by manipulating a parameter through API request URL which could lead to unauthorized access to sensitive information belonging to other users.	6.5	More Details
CVE-2024-38231	Windows Remote Desktop Licensing Service Denial of Service Vulnerability	6.5	More Details
CVE-2024-45096	IBM Aspera Faspex 5.0.0 through 5.0.9 could allow a user with access to the package to obtain sensitive information through a directory listing.	6.5	More Details
CVE-2024-7688	The AZIndex WordPress plugin through 0.8.1 does not have CSRF checks in some places, which could allow attackers to make logged in admin delete arbitrary indexes via a CSRF attack	6.5	More Details
CVE-2024-38230	Windows Standards-Based Storage Management Service Denial of Service Vulnerability	6.5	More Details
CVE-2024-38235	Windows Hyper-V Denial of Service Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43466	Microsoft SharePoint Server Denial of Service Vulnerability	6.5	More Details
CVE-2024-43482	Microsoft Outlook for iOS Information Disclosure Vulnerability	6.5	More Details
CVE-2024-8106	The The Ultimate WordPress Toolkit – WP Extended plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.0.8 via the download_user_ajax function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to extract sensitive data including usernames, hashed passwords, and emails.	6.5	More Details
CVE-2024-6894	The RD Station plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 5.3.2 due to insufficient input sanitization and output escaping of post metaboxes added by the plugin. 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-2024-6929	The Dynamic Featured Image plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘dfiFeatured’ parameter in all versions up to, and including, 3.7.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-8317	The WP AdCenter – Ad Manager & Adsense Ads plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘ad_alignment’ attribute in all versions up to, and including, 2.5.6 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-2024-8363	The Share This Image plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's STI Buttons shortcode in all versions up to, and including, 2.02 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-2024-8241	The Nova Blocks by Pixelgrade plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'align' attribute of the 'wp:separator' Gutenberg block in all versions up to, and including, 2.1.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-8325	The Blockspare: Gutenberg Blocks & Patterns for Blogs, Magazines, Business Sites – Post Grids, Sliders, Carousels, Counters, Page Builder & Starter Site Imports, No Coding Needed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several parameters in the ‘blockspare_render_social_sharing_block’ function in all versions up to, and including, 3.2.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-45393	Computer Vision Annotation Tool (CVAT) is an interactive video and image annotation tool for computer vision. An attacker with a CVAT account can access webhook delivery information for any webhook registered on the CVAT instance, including that of other users. For each delivery, this contains information about the event that caused the delivery, typically including full details about the object on which an action was performed (such as the task for an "update:task" event), and the user who performed the action. In addition, the attacker can redeliver any past delivery of any webhook, and trigger a ping event for any webhook. Upgrade to CVAT 2.18.0 or any later version.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8318	The Attributes for Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘attributesForBlocks’ parameter in all versions up to, and including, 1.0.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-6849	The Preloader Plus – WordPress Loading Screen Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 2.2.1 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-2024-8543	The Slider comparison image before and after plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's [sciba] shortcode in all versions up to, and including, 0.8.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-7599	The Advanced Sermons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘sermon_video_embed’ parameter in all versions up to, and including, 3.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-7611	The Enter Addons – Ultimate Template Builder for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tag' attribute of the Events Card widget in all versions up to, and including, 2.1.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-8574	A vulnerability has been found in TOTOLINK AC1200 T8 4.1.5cu.861_B20230220 and classified as critical. This vulnerability affects the function setParentalRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument slaveIpList leads to os command 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.	6.3	More Details
CVE-2024-42759	An issue in Ellevo v.6.2.0.38160 allows a remote attacker to escalate privileges via the /api/usuario/cadastrodesuplente endpoint.	6.3	More Details
CVE-2024-8560	A vulnerability, which was classified as critical, was found in SourceCodester Simple Invoice Generator System 1.0. Affected is an unknown function of the file /save_invoice.php. The manipulation of the argument invoice_code/customer/cashier/total_amount/discount_percentage/discount_amount/tendered_amount 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-2024-8561	A vulnerability has been found in SourceCodester PHP CRUD 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /endpoint/delete.php of the component Delete Person Handler. The manipulation of the argument person leads to sql injection. The attack can be launched remotely.	6.3	More Details
CVE-2024-8473	Cross-Site Scripting (XSS) vulnerability, whereby user-controlled input is not sufficiently encrypted. Exploitation of this vulnerability could allow an attacker to retrieve the session details of an authenticated user through user_email parameter in /jobportal/admin/login.php.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8472	Cross-Site Scripting (XSS) vulnerability, whereby user-controlled input is not sufficiently encrypted. Exploitation of this vulnerability could allow an attacker to retrieve the session details of an authenticated user through multiple parameters in /jobportal/index.php.	6.3	More Details
CVE-2024-8564	A vulnerability was found in SourceCodester PHP CRUD 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /endpoint/update.php. The manipulation of the argument tbl_person_id/first_name/middle_name/last_name 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-2024-8471	Cross-Site Scripting (XSS) vulnerability, whereby user-controlled input is not sufficiently encrypted. Exploitation of this vulnerability could allow an attacker to retrieve the session details of an authenticated user through JOBID and USERNAME parameters in /jobportal/process.php.	6.3	More Details
CVE-2024-8415	A vulnerability was found in SourceCodester Food Ordering Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /routers/add-ticket.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-8568	A vulnerability, which was classified as critical, was found in Mini-Tmall up to 20240901. Affected is the function rewardMapper.select of the file tmall/admin/order/1/1. The manipulation of the argument orderBy 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-2024-27122	A cross-site scripting (XSS) vulnerability has been reported to affect Notes Station 3. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions: Notes Station 3 3.9.6 and later	6.3	More Details
CVE-2024-27126	A cross-site scripting (XSS) vulnerability has been reported to affect Notes Station 3. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions: Notes Station 3 3.9.6 and later	6.3	More Details
CVE-2024-8611	A vulnerability classified as critical was found in itsourcecode Tailoring Management System 1.0. Affected by this vulnerability is an unknown functionality of the file ssms.php. The manipulation of the argument customer leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-5957	This vulnerability allows unauthenticated remote attackers to bypass authentication and gain APIs access of the Manager.	6.3	More Details
CVE-2024-8416	A vulnerability was found in SourceCodester Food Ordering Management System 1.0. It has been classified as critical. This affects an unknown part of the file /routers/ticket-status.php. The manipulation of the argument ticket_id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-8408	A vulnerability was found in Linksys WRT54G 4.21.5. It has been rated as critical. Affected by this issue is the function validate_services_port of the file /apply.cgi of the component POST Parameter Handler. The manipulation of the argument services_array leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-8557	A vulnerability classified as critical has been found in SourceCodester Food Ordering Management System 1.0. This affects an unknown part of the file /foms/routers/cancel-order.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8570	A vulnerability was found in itsourcecode Tailoring Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /inccatadd.php. The manipulation of the argument title leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-34637	Improper access control in WindowManagerService prior to SMR Sep-2024 Release 1 in Android 12, and SMR Jun-2024 Release 1 in Android 13 and Android 14 allows local attackers to bypass restrictions on starting services from the background.	6.2	More Details
CVE-2024-34651	Improper authorization in My Files prior to SMR Sep-2024 Release 1 allows local attackers to access restricted data in My Files.	6.2	More Details
CVE-2024-34654	Improper Export of android application component in My Files prior to SMR Sep-2024 Release 1 allows local attackers to access files with My Files' privilege.	6.2	More Details
CVE-2024-34655	Incorrect use of privileged API in UniversalCredentialManager prior to SMR Sep-2024 Release 1 allows local attackers to access privileged API related to UniversalCredentialManager.	6.2	More Details
CVE-2024-45039	gnark is a fast zk-SNARK library that offers a high-level API to design circuits. Versions prior to 0.11.0 have a soundness issue - in case of multiple commitments used inside the circuit the prover is able to choose all but the last commitment. As gnark uses the commitments for optimized non-native multiplication, lookup checks etc. as random challenges, then it could impact the soundness of the whole circuit. However, using multiple commitments has been discouraged due to the additional cost to the verifier and it has not been supported in the recursive in-circuit Groth16 verifier and Solidity verifier. gnark's maintainers expect the impact of the issue be very small - only for the users who have implemented the native Groth16 verifier or are using it with multiple commitments. We do not have information of such users. The issue has been patched in version 0.11.0. As a workaround, users should follow gnark maintainers' recommendation to use only a single commitment and then derive in-circuit commitments as needed using the `std/multicommit` package.	6.2	More Details
CVE-2024-45441	Input verification vulnerability in the system service module Impact: Successful exploitation of this vulnerability will affect availability.	6.2	More Details
CVE-2024-8298	Memory request vulnerability in the memory management module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	6.2	More Details
CVE-2024-42423	Citrix Workspace App version 23.9.0.24.4 on Dell ThinOS 2311 contains an Incorrect Authorization vulnerability when Citrix CEB is enabled for WebLogin. A local unauthenticated user with low privileges may potentially exploit this vulnerability to bypass existing controls and perform unauthorized actions leading to information disclosure and tampering.	6.1	More Details
CVE-2024-45429	Cross-site scripting vulnerability exists in Advanced Custom Fields versions 6.3.5 and earlier and Advanced Custom Fields Pro versions 6.3.5 and earlier. If an attacker with the 'capability' setting privilege which is set in the product settings stores an arbitrary script in the field label, the script may be executed on the web browser of the logged-in user with the same privilege as the attacker's.	6.1	More Details
CVE-2024-34831	cross-site scripting (XSS) vulnerability in Gibbon Core v26.0.00 allows an attacker to execute arbitrary code via the imageLink parameter in the library_manage_catalog_editProcess.php component.	6.1	More Details
CVE-2024-8586	WebITR from Uniong has an Open Redirect vulnerability, which allows unauthorized remote attackers to exploit this vulnerability to forge URLs. Users, believing they are accessing a trusted domain, can be redirected to another page, potentially leading to phishing attacks.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45625	Cross-site scripting vulnerability exists in Forminator versions prior to 1.34.1. If this vulnerability is exploited, an arbitrary script may be executed on the web browser of the user who follows a crafted URL and accesses the webpage with the web form created by Forminator.	6.1	More Details
CVE-2024-6020	The Sign-up Sheets WordPress plugin before 2.2.13 does not escape some generated URLs, as well as the $_SERVER['REQUEST_URI'] parameter before outputting them back in attributes, which could lead to Reflected Cross-Site Scripting.	6.1	More Details
CVE-2024-7784	During internal Axis Security Development Model (ASDM) threat-modelling, a flaw was found in the protection for device tampering (commonly known as Secure Boot) in AXIS OS making it vulnerable to a sophisticated attack to bypass this protection. To Axis' knowledge, there are no known exploits of the vulnerability at this time. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution.	6.1	More Details
CVE-2024-42341	Loway - CWE-601: URL Redirection to Untrusted Site ('Open Redirect')	6.1	More Details
CVE-2024-20506	A vulnerability in the ClamD service module of Clam AntiVirus (ClamAV) versions 1.4.0, 1.3.2 and prior versions, all 1.2.x versions, 1.0.6 and prior versions, all 0.105.x versions, all 0.104.x versions, and 0.103.11 and all prior versions could allow an authenticated, local attacker to corrupt critical system files. The vulnerability is due to allowing the ClamD process to write to its log file while privileged without checking if the logfile has been replaced with a symbolic link. An attacker could exploit this vulnerability if they replace the ClamD log file with a symlink to a critical system file and then find a way to restart the ClamD process. An exploit could allow the attacker to corrupt a critical system file by appending ClamD log messages after restart.	6.1	More Details
CVE-2024-24510	Cross Site Scripting vulnerability in Alinto SOGo before 5.10.0 allows a remote attacker to execute arbitrary code via the import function to the mail component.	6.1	More Details
CVE-2024-44872	A reflected cross-site scripting (XSS) vulnerability in moziloCMS v3.0 allows attackers to execute arbitrary code in the context of a user's browser via injecting a crafted payload.	6.1	More Details
CVE-2024-34645	Improper input validation in ThemeCenter prior to SMR Sep-2024 Release 1 allows physical attackers to install privileged applications.	6.1	More Details
CVE-2023-50883	ONLYOFFICE Docs before 8.0.1 allows XSS because a macro is an immediately-invoked function expression (IIFE), and therefore a sandbox escape is possible by directly calling the constructor of the Function object. NOTE: this issue exists because of an incorrect fix for CVE-2021-43446.	6.1	More Details
CVE-2024-7260	An open redirect vulnerability was found in Keycloak. A specially crafted URL can be constructed where the referrer and referrer_uri parameters are made to trick a user to visit a malicious webpage. A trusted URL can trick users and automation into believing that the URL is safe, when, in fact, it redirects to a malicious server. This issue can result in a victim inadvertently trusting the destination of the redirect, potentially leading to a successful phishing attack or other types of attacks. Once a crafted URL is made, it can be sent to a Keycloak admin via email for example. This will trigger this vulnerability when the user visits the page and clicks the link. A malicious actor can use this to target users they know are Keycloak admins for further attacks. It may also be possible to bypass other domain-related security checks, such as supplying this as a OAuth redirect uri. The malicious actor can further obfuscate the redirect_uri using URL encoding, to hide the text of the actual malicious website domain.	6.1	More Details
CVE-2024-44819	Cross Site Scripting vulnerability in ZZCMS v.2023 and before allows a remote attacker to obtain sensitive information via a crafted script to the pagename parameter of the admin/del.php component.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45279	Due to insufficient input validation, CRM Blueprint Application Builder Panel of SAP NetWeaver Application Server for ABAP allows an unauthenticated attacker to craft a URL link which could embed a malicious JavaScript. When a victim clicks on this link, the script will be executed in the victim's browser giving the attacker the ability to access and/or modify information with no effect on availability of the application.	6.1	More Details
CVE-2024-44820	A sensitive information disclosure vulnerability exists in ZZCMS v.2023 and before within the eginfo.php file located at /3/E_bak5.1/upload/. When accessed with the query parameter phome=ShowPHPInfo, the application executes the phpinfo() function, which exposes detailed information about the PHP environment, including server configuration, loaded modules, and environment variables.	6.1	More Details
CVE-2024-44728	Sourcecodehero Event Management System 1.0 allows Stored Cross-Site Scripting via parameters Full Name, Address, Email, and contact# in /clientdetails/admin/regester.php.	6.1	More Details
CVE-2024-44085	ONLYOFFICE Docs before 8.1.0 allows XSS via a GeneratorFunction Object attack against a macro. This is related to use of an immediately-invoked function expression (IIFE) for a macro. NOTE: this issue exists because of an incorrect fix for CVE-2021-43446 and CVE-2023-50883.	6.1	More Details
CVE-2024-8119	The The Ultimate WordPress Toolkit – WP Extended plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the page parameter in all versions up to, and including, 3.0.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-8117	The The Ultimate WordPress Toolkit – WP Extended plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘selected_option’ parameter in all versions up to, and including, 3.0.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-42378	Due to weak encoding of user-controlled inputs, eProcurement on SAP S/4HANA allows malicious scripts to be executed in the application, potentially leading to a Reflected Cross-Site Scripting (XSS) vulnerability. This has no impact on the availability of the application, but it can have some minor impact on its confidentiality and integrity.	6.1	More Details
CVE-2024-45443	Directory traversal vulnerability in the cust module Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	6.1	More Details
CVE-2024-45595	D-Tale is a visualizer for Pandas data structures. Users hosting D-Tale publicly can be vulnerable to remote code execution allowing attackers to run malicious code on the server. Users should upgrade to version 3.14.1 where the "Custom Filter" input is turned off by default.	6.1	More Details
CVE-2024-7077	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Semtek Informatics Software Consulting Inc. Semtek Sempos allows Reflected XSS.This issue affects Semtek Sempos: through 31072024.	6.1	More Details
CVE-2024-45176	An issue was discovered in za-internet C-MOR Video Surveillance 5.2401. Due to improper input validation, the C-MOR web interface is vulnerable to reflected cross-site scripting (XSS) attacks. It was found out that different functions are prone to reflected cross-site scripting attacks due to insufficient user input validation.	6.1	More Details
CVE-2024-45400	ckeditor-plugin-openlink is a plugin for the CKEditor JavaScript text editor that extends the context menu with a possibility to open a link in a new tab. A vulnerability in versions of the plugin prior to 1.0.7 allowed a user to execute JavaScript code by abusing the link href attribute. The fix is available starting with version 1.0.7.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45405	\`gix-path\` is a crate of the \`gitoxide\` project (an implementation of \`git\` written in Rust) dealing paths and their conversions. Prior to version 0.10.11, \`gix-path\` runs \`git\` to find the path of a configuration file associated with the \`git\` installation, but improperly resolves paths containing unusual or non-ASCII characters, in rare cases enabling a local attacker to inject configuration leading to code execution. Version 0.10.11 contains a patch for the issue. In \`gix_path::env\`, the underlying implementation of the \`installation_config\` and \`installation_config_prefix\` functions calls \`git config -l --show-origin\` to find the path of a file to treat as belonging to the \`git\` installation. Affected versions of \`gix-path\` do not pass \`-z\`/\`--null\` to cause \`git\` to report literal paths. Instead, to cover the occasional case that \`git\` outputs a quoted path, they attempt to parse the path by stripping the quotation marks. The problem is that, when a path is quoted, it may change in substantial ways beyond the concatenation of quotation marks. If not reversed, these changes can result in another valid path that is not equivalent to the original. On a single-user system, it is not possible to exploit this, unless \`GIT_CONFIG_SYSTEM\` and \`GIT_CONFIG_GLOBAL\` have been set to unusual values or Git has been installed in an unusual way. Such a scenario is not expected. Exploitation is unlikely even on a multi-user system, though it is plausible in some uncommon configurations or use cases. In general, exploitation is more likely to succeed if users are expected to install \`git\` themselves, and are likely to do so in predictable locations; locations where \`git\` is installed, whether due to usernames in their paths or otherwise, contain characters that \`git\` quotes by default in paths, such as non-English letters and accented letters; a custom \`system\`-scope configuration file is specified with the \`GIT_CONFIG_SYSTEM\` environment variable, and its path is in an unusual location or has strangely named components; or a \`system\`-scope configuration file is absent, empty, or suppressed by means other than \`GIT_CONFIG_NOSYSTEM\`. Currently, \`gix-path\` can treat a \`global\`-scope configuration file as belonging to the installation if no higher scope configuration file is available. This increases the likelihood of exploitation even on a system where \`git\` is installed system-wide in an ordinary way. However, exploitation is expected to be very difficult even under any combination of those factors.	6.0	More Details
CVE-2024-45283	SAP NetWeaver AS for Java allows an authorized attacker to obtain sensitive information. The attacker could obtain the username and password when creating an RFC destination. After successful exploitation, an attacker can read the sensitive information but cannot modify or delete the data.	6.0	More Details
CVE-2024-20469	A vulnerability in specific CLI commands in Cisco Identity Services Engine (ISE) could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have valid Administrator privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root.	6.0	More Details
CVE-2024-21528	All versions of the package node-gettext are vulnerable to Prototype Pollution via the addTranslations() function in gettext.js due to improper user input sanitization.	5.9	More Details
CVE-2024-45751	tgt (aka Linux target framework) before 1.0.93 attempts to achieve entropy by calling rand without srand. The PRNG seed is always 1, and thus the sequence of challenges is always identical.	5.9	More Details
CVE-2024-45589	RapidIdentity LTS through 2023.0.2 and Cloud through 2024.08.0 improperly restricts excessive authentication attempts and allows a remote attacker to cause a denial of service via the username parameters.	5.9	More Details
CVE-2024-25074	An issue was discovered in Samsung Semiconductor Mobile Processor and Modem Exynos 9820, Exynos 9825, Exynos 980, Exynos 990, Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 9110, Exynos W920, Exynos W930, Exynos Modem 5123, Exynos Modem 5300. The baseband software does not properly check a pointer specified by the SM (Session Management module), which can lead to Denial of Service (Untrusted Pointer Dereference).	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30756	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-7 LTE (All versions < V3.5.20), SIMATIC CP 1243-8 IRC (6GK7243-8RX30-0XE0) (All versions < V3.5.20), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC IPC DiagBase (All versions), SIMATIC IPC DiagMonitor (All versions), SIMATIC WinCC Runtime Advanced (All versions), SIPLUS TIM 1531 IRC (6AG1543-1MX00-7XE0) (All versions < V2.4.8), TIM 1531 IRC (6GK7543-1MX00-0XE0) (All versions < V2.4.8). The web server of the affected devices do not properly handle certain errors when using the Expect HTTP request header, resulting in NULL dereference. This could allow a remote attacker with no privileges to cause a denial of service condition in the system.	5.9	More Details
CVE-2023-28827	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-7 LTE (All versions < V3.5.20), SIMATIC CP 1243-8 IRC (6GK7243-8RX30-0XE0) (All versions < V3.5.20), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC IPC DiagBase (All versions), SIMATIC IPC DiagMonitor (All versions), SIMATIC WinCC Runtime Advanced (All versions), SIPLUS TIM 1531 IRC (6AG1543-1MX00-7XE0) (All versions < V2.4.8), TIM 1531 IRC (6GK7543-1MX00-0XE0) (All versions < V2.4.8). The web server of the affected devices do not properly handle certain requests, causing a timeout in the watchdog, which could lead to the clean up of pointers. This could allow a remote attacker to cause a denial of service condition in the system.	5.9	More Details
CVE-2024-21904	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later	5.9	More Details
CVE-2024-37068	IBM Maximo Application Suite - Manage Component 8.10, 8.11, and 9.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information using man in the middle techniques.	5.9	More Details
CVE-2024-45040	gnark is a fast zk-SNARK library that offers a high-level API to design circuits. Prior to version 0.11.0, commitments to private witnesses in Groth16 as implemented break the zero-knowledge property. The vulnerability affects only Groth16 proofs with commitments. Notably, PLONK proofs are not affected. The vulnerability affects the zero-knowledge property of the proofs - in case the witness (secret or internal) values are small, then the attacker may be able to enumerate all possible choices to deduce the actual value. If the possible choices for the variables to be committed is large or there are many values committed, then it would be computationally infeasible to enumerate all valid choices. It doesn't affect the completeness/soundness of the proofs. The vulnerability has been fixed in version 0.11.0. The patch to fix the issue is to add additional randomized value to the list of committed value at proving time to mask the rest of the values which were committed. As a workaround, the user can manually commit to a randomized value.	5.9	More Details
CVE-2024-45097	IBM Aspera Faspex 5.0.0 through 5.0.9 could allow a user to bypass intended access restrictions and conduct resource modification.	5.9	More Details
CVE-2024-25073	An issue was discovered in Samsung Semiconductor Mobile Processor and Modem Exynos 9820, Exynos 9825, Exynos 980, Exynos 990, Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 9110, Exynos W920, Exynos W930, Exynos Modem 5123, Exynos Modem 5300. The baseband software does not properly check a pointer specified by the CC (Call Control module), which can lead to Denial of Service (Untrusted Pointer Dereference).	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8321	Missing authentication in Network Isolation of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to isolate managed devices from the network.	5.8	More Details
CVE-2024-45281	SAP BusinessObjects Business Intelligence Platform allows a high privilege user to run client desktop applications even if some of the DLLs are not digitally signed or if the signature is broken. The attacker needs to have local access to the vulnerable system to perform DLL related tasks. This could result in a high impact on confidentiality and integrity of the application.	5.8	More Details
CVE-2024-8445	The fix for CVE-2024-2199 in 389-ds-base was insufficient to cover all scenarios. In certain product versions, an authenticated user may cause a server crash while modifying \`userPassword\` using malformed input.	5.7	More Details
CVE-2024-7698	A low privileged remote attacker can get access to CSRF tokens of higher privileged users which can be abused to mount CSRF attacks.	5.7	More Details
CVE-2024-44072	OS command injection vulnerability exists in BUFFALO wireless LAN routers and wireless LAN repeaters. If a user logs in to the management page and sends a specially crafted request to the affected product from the product's specific management page, an arbitrary OS command may be executed.	5.7	More Details
CVE-2024-42491	Asterisk is an open-source private branch exchange (PBX). Prior to versions 18.24.3, 20.9.3, and 21.4.3 of Asterisk and versions 18.9-cert12 and 20.7-cert2 of certified-asterisk, if Asterisk attempts to send a SIP request to a URI whose host portion starts with \`.1\` or \`[.1]\`, and res_resolver_unbound is loaded, Asterisk will crash with a SEGV. To receive a patch, users should upgrade to one of the following versions: 18.24.3, 20.9.3, 21.4.3, certified-18.9-cert12, certified-20.7-cert2. Two workarounds are available. Disable res_resolver_unbound by setting \`noload = res_resolver_unbound.so\` in modules.conf, or set \`rewrite_contact = yes\` on all PJSIP endpoints. NOTE: This may not be appropriate for all Asterisk configurations.	5.7	More Details
CVE-2024-45446	Access permission verification vulnerability in the camera driver module Impact: Successful exploitation of this vulnerability will affect availability.	5.5	More Details
CVE-2024-45444	Access permission verification vulnerability in the WMS module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	5.5	More Details
CVE-2024-45406	Craft is a content management system (CMS). Craft CMS 5 stored XSS can be triggered by the breadcrumb list and title fields with user input.	5.5	More Details
CVE-2024-44955	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Don't refer to dc_sink in is_dsc_need_re_compute [Why] When unplug one of monitors connected after mst hub, encounter null pointer dereference. It's due to dc_sink get released immediately in early_unregister() or detect_ctx(). When commit new state which directly referring to info stored in dc_sink will cause null pointer dereference. [how] Remove redundant checking condition. Relevant condition should already be covered by checking if dsc_aux is null or not. Also reset dsc_aux to NULL when the connector is disconnected.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44956	In the Linux kernel, the following vulnerability has been resolved: drm/xe/preempt_fence: enlarge the fence critical section It is really easy to introduce subtle deadlocks in preempt_fence_work_func() since we operate on single global ordered-wq for signalling our preempt fences behind the scenes, so even though we signal a particular fence, everything in the callback should be in the fence critical section, since blocking in the callback will prevent other published fences from signalling. If we enlarge the fence critical section to cover the entire callback, then lockdep should be able to understand this better, and complain if we grab a sensitive lock like vm->lock, which is also held when waiting on preempt fences.	5.5	More Details
CVE-2024-43781	A vulnerability has been identified in SINUMERIK 828D V4 (All versions < V4.95 SP3), SINUMERIK 840D sl V4 (All versions < V4.95 SP3 in connection with using Create MyConfig (CMC) <= V4.8 SP1 HF6), SINUMERIK ONE (All versions < V6.23 in connection with using Create MyConfig (CMC) <= V6.6), SINUMERIK ONE (All versions < V6.15 SP4 in connection with using Create MyConfig (CMC) <= V6.6). Affected systems, that have been provisioned with Create MyConfig (CMC), contain a Insertion of Sensitive Information into Log File vulnerability. This could allow a local authenticated user with low privileges to read sensitive information and thus circumvent access restrictions.	5.5	More Details
CVE-2024-44953	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: core: Fix deadlock during RTC update There is a deadlock when runtime suspend waits for the flush of RTC work, and the RTC work calls ufshcd_rpm_get_sync() to wait for runtime resume. Here is deadlock backtrace: kworker/0:1 D 4892.876354 10 10971 4859 0x4208060 0x8 10 0 120 670730152367 ptr f0ffff80c2e40000 0 1 0x00000001 0x000000ff 0x000000ff 0x000000ff <ffffffee5e71ddb0> __switch_to+0x1a8/0x2d4 <ffffffee5e71e604> __schedule+0x684/0xa98 <ffffffee5e71ea60> schedule+0x48/0xc8 <ffffffee5e725f78> schedule_timeout+0x48/0x170 <ffffffee5e71fb74> do_wait_for_common+0x108/0x1b0 <ffffffee5e71efe0> wait_for_completion+0x44/0x60 <ffffffee5d6de968> __flush_work+0x39c/0x424 <ffffffee5d6decc0> __cancel_work_sync+0xd8/0x208 <ffffffee5d6dee2c> cancel_delayed_work_sync+0x14/0x28 <ffffffee5e2551b8> __ufshcd_wl_suspend+0x19c/0x480 <ffffffee5e255fb8> ufshcd_wl_runtime_suspend+0x3c/0x1d4 <ffffffee5dffd80c> scsi_runtime_suspend+0x78/0xc8 <ffffffee5df93580> __rpm_callback+0x94/0x3e0 <ffffffee5df90b0c> rpm_suspend+0x2d4/0x65c <ffffffee5df91448> __pm_runtime_suspend+0x80/0x114 <ffffffee5dffd95c> scsi_runtime_idle+0x38/0x6c <ffffffee5df912f4> rpm_idle+0x264/0x338 <ffffffee5df90f14> __pm_runtime_idle+0x80/0x110 <ffffffee5e24ce44> ufshcd_rtc_work+0x128/0x1e4 <ffffffee5d6e3a40> process_one_work+0x26c/0x650 <ffffffee5d6e65c8> worker_thread+0x260/0x3d8 <ffffffee5d6edec8> kthread+0x110/0x134 <ffffffee5d616b18> ret_from_fork+0x10/0x20 Skip updating RTC if RPM state is not RPM_ACTIVE.	5.5	More Details
CVE-2024-45002	In the Linux kernel, the following vulnerability has been resolved: rtla/osnoise: Prevent NULL dereference in error handling If the "tool->data" allocation fails then there is no need to call osnoise_free_top() and, in fact, doing so will lead to a NULL dereference.	5.5	More Details
CVE-2024-8645	SPRT dissector crash in Wireshark 4.2.0 to 4.0.5 and 4.0.0 to 4.0.15 allows denial of service via packet injection or crafted capture file	5.5	More Details
CVE-2024-44971	In the Linux kernel, the following vulnerability has been resolved: net: dsa: bcm_sf2: Fix a possible memory leak in bcm_sf2_mdio_register() bcm_sf2_mdio_register() calls of_phy_find_device() and then phy_device_remove() in a loop to remove existing PHY devices. of_phy_find_device() eventually calls bus_find_device(), which calls get_device() on the returned struct device * to increment the refcount. The current implementation does not decrement the refcount, which causes memory leak. This commit adds the missing phy_device_free() call to decrement the refcount via put_device() to balance the refcount.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52915	In the Linux kernel, the following vulnerability has been resolved: media: dvb-usb-v2: af9035: Fix null-ptr-deref in af9035_i2c_master_xfer In af9035_i2c_master_xfer, msg is controlled by user. When msg[i].buf is null and msg[i].len is zero, former checks on msg[i].buf would be passed. Malicious data finally reach af9035_i2c_master_xfer. If accessing msg[i].buf[0] without sanity check, null ptr deref would happen. We add check on msg[i].len to prevent crash. Similar commit: commit 0ed554fd769a ("media: dvb-usb: az6027: fix null-ptr-deref in az6027_i2c_xfer()")	5.5	More Details
CVE-2024-44975	In the Linux kernel, the following vulnerability has been resolved: cgroup/cpuset: fix panic caused by partcmd_update We find a bug as below: BUG: unable to handle page fault for address: 00000003 PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 3 PID: 358 Comm: bash Tainted: G W I 6.6.0-10893-g60d6 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/4 RIP: 0010:partition_sched_domains_locked+0x483/0x600 Code: 01 48 85 d2 74 0d 48 83 05 29 3f f8 03 01 f3 48 0f bc c2 89 c0 48 9 RSP: 0018:ffffc90000fdbc58 EFLAGS: 00000202 RAX: 0000000100000003 RBX: ffff888100b3dfa0 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 000000000002fe80 RBP: ffff888100b3dfb0 R08: 0000000000000001 R09: 0000000000000000 R10: ffffc90000fdbcb0 R11: 0000000000000004 R12: 0000000000000002 R13: ffff888100a92b48 R14: 0000000000000000 R15: 0000000000000000 FS: 00007f44a5425740(0000) GS:ffff888237d80000(0000) knlGS:0000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000100030973 CR3: 000000010722c000 CR4: 00000000000006e0 Call Trace: <TASK> ? show_regs+0x8c/0xa0 ? __die_body+0x23/0xa0 ? __die+0x3a/0x50 ? page_fault_oops+0x1d2/0x5c0 ? partition_sched_domains_locked+0x483/0x600 ? search_module_extables+0x2a/0xb0 ? search_exception_tables+0x67/0x90 ? kernelmode_fixup_or_oops+0x144/0x1b0 ? __bad_area_nosemaphore+0x211/0x360 ? up_read+0x3b/0x50 ? bad_area_nosemaphore+0x1a/0x30 ? exc_page_fault+0x890/0xd90 ? __lock_acquire.constprop.0+0x24f/0x8d0 ? __lock_acquire.constprop.0+0x24f/0x8d0 ? asm_exc_page_fault+0x26/0x30 ? partition_sched_domains_locked+0x483/0x600 ? partition_sched_domains_locked+0xf0/0x600 rebuild_sched_domains_locked+0x806/0xdc0 update_partition_sd_lb+0x118/0x130 cpuset_write_resmask+0xffc/0x1420 cgroup_file_write+0xb2/0x290 kernfs_fop_write_iter+0x194/0x290 new_sync_write+0xeb/0x160 vfs_write+0x16f/0x1d0 ksys_write+0x81/0x180 __x64_sys_write+0x21/0x30 x64_sys_call+0x2f25/0x4630 do_syscall_64+0x44/0xb0 entry_SYSCALL_64_after_hwframe+0x78/0xe2 RIP: 0033:0x7f44a553c887 It can be reproduced with cammands: cd /sys/fs/cgroup/ mkdir test cd test/ echo +cpuset > ../cgroup.subtree_control echo root > cpuset.cpus.partition cat /sys/fs/cgroup/cpuset.cpus.effective 0-3 echo 0-3 > cpuset.cpus // taking away all cpus from root This issue is caused by the incorrect rebuilding of scheduling domains. In this scenario, test/cpuset.cpus.partition should be an invalid root and should not trigger the rebuilding of scheduling domains. When calling update_parent_effective_cpumask with partcmd_update, if newmask is not null, it should recheck newmask whether there are cpus is available for parect/cs that has tasks.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44976	In the Linux kernel, the following vulnerability has been resolved: ata: pata_macio: Fix DMA table overflow Kolbjørn and Jonáš reported that their 32-bit PowerMacs were crashing in pata-macio since commit 09fe2bfa6b83 ("ata: pata_macio: Fix max_segment_size with PAGE_SIZE == 64K"). For example: kernel BUG at drivers/ata/pata_macio.c:544! Oops: Exception in kernel mode, sig: 5 [#1] BE PAGE_SIZE=4K MMU=Hash SMP NR_CPUS=2 DEBUG_PAGEALLOC PowerMac ... NIP pata_macio_qc_prep+0xf4/0x190 LR pata_macio_qc_prep+0xfc/0x190 Call Trace: 0xc1421660 (unreliable) ata_qc_issue+0x14c/0x2d4 __ata_scsi_queuecmd+0x200/0x53c ata_scsi_queuecmd+0x50/0xe0 scsi_queue_rq+0x788/0xb1c __blk_mq_issue_directly+0x58/0xf4 blk_mq_plug_issue_direct+0x8c/0x1b4 blk_mq_flush_plug_list.part.0+0x584/0x5e0 __blk_flush_plug+0xf8/0x194 __submit_bio+0x1b8/0x2e0 submit_bio_noacct_nocheck+0x230/0x304 btrfs_work_helper+0x200/0x338 process_one_work+0x1a8/0x338 worker_thread+0x364/0x4c0 kthread+0x100/0x104 start_kernel_thread+0x10/0x14 That commit increased max_segment_size to 64KB, with the justification that the SCSI core was already using that size when PAGE_SIZE == 64KB, and that there was existing logic to split over-sized requests. However with a sufficiently large request, the splitting logic causes each sg to be split into two commands in the DMA table, leading to overflow of the DMA table, triggering the BUG_ON(). With default settings the bug doesn't trigger, because the request size is limited by max_sectors_kb == 1280, however max_sectors_kb can be increased, and apparently some distros do that by default using udev rules. Fix the bug for 4KB kernels by reverting to the old max_segment_size. For 64KB kernels the sg_tablesize needs to be halved, to allow for the possibility that each sg will be split into two.	5.5	More Details
CVE-2024-44979	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Fix missing workqueue destroy in xe_gt_pagefault On driver reload we never free up the memory for the pagefault and access counter workqueues. Add those destroy calls here. (cherry picked from commit 7586fc52b14e0b8edd0d1f8a434e0de2078b7b2b)	5.5	More Details
CVE-2024-44980	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Fix opregion leak Being part o the display, ideally the setup and cleanup would be done by display itself. However this is a bigger refactor that needs to be done on both i915 and xe. For now, just fix the leak: unreferenced object 0xffff8881a0300008 (size 192): comm "modprobe", pid 4354, jiffies 4295647021 hex dump (first 32 bytes): 00 00 87 27 81 88 ff ff 18 80 9b 00 00 c9 ff ff ...'........... 18 81 9b 00 00 c9 ff ff 00 00 00 00 00 00 00 00 .... backtrace (crc 99260e31): [<ffffffff823ce65b>] kmemleak_alloc+0x4b/0x80 [<ffffffff81493be2>] kmalloc_trace_noprof+0x312/0x3d0 [<ffffffffa1345679>] intel_opregion_setup+0x89/0x700 [xe] [<ffffffffa125bfaf>] xe_display_init_noirq+0x2f/0x90 [xe] [<ffffffffa1199ec3>] xe_device_probe+0x7a3/0xbf0 [xe] [<ffffffffa11f3713>] xe_pci_probe+0x333/0x5b0 [xe] [<ffffffff81af6be8>] local_pci_probe+0x48/0xb0 [<ffffffff81af8778>] pci_device_probe+0xc8/0x280 [<ffffffff81d09048>] really_probe+0xf8/0x390 [<ffffffff81d0937a>] __driver_probe_device+0x8a/0x170 [<ffffffff81d09503>] driver_probe_device+0x23/0xb0 [<ffffffff81d097b7>] __driver_attach+0xc7/0x190 [<ffffffff81d0628d>] bus_for_each_dev+0x7d/0xd0 [<ffffffff81d0851e>] driver_attach+0x1e/0x30 [<ffffffff81d07ac7>] bus_add_driver+0x117/0x250 (cherry picked from commit 6f4e43a2f771b737d991142ec4f6d4b7ff31fbb4)	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44981	In the Linux kernel, the following vulnerability has been resolved: workqueue: Fix UBSAN 'subtraction overflow' error in shift_and_mask() UBSAN reports the following 'subtraction overflow' error when booting in a virtual machine on Android: | Internal error: UBSAN: integer subtraction overflow: 00000000f2005515 [#1] PREEMPT SMP | Modules linked in: | CPU: 0 PID: 1 Comm: swapper/0 Not tainted 6.10.0-00006-g3cbe9e5abd46-dirty #4 | Hardware name: linux,dummy-virt (DT) | pstate: 600000c5 (nZCv daIF -PAN -UAO -TCO -DIT -SSBS BTYPE=--) | pc : cancel_delayed_work+0x34/0x44 | lr : cancel_delayed_work+0x2c/0x44 | sp : ffff80008002ba60 | x29: ffff80008002ba60 x28: 0000000000000000 x27: 0000000000000000 | x26: 0000000000000000 x25: 0000000000000000 x24: 0000000000000000 | x23: 0000000000000000 x22: 0000000000000000 x21: ffff1f65014cd3c0 | x20: ffffc0e84c9d0da0 x19: ffffc0e84cab3558 x18: ffff800080009058 | x17: 00000000247ee1f8 x16: 00000000247ee1f8 x15: 00000000bdcb279d | x14: 0000000000000001 x13: 0000000000000075 x12: 00000a0000000000 | x11: ffff1f6501499018 x10: 00984901651fffff x9 : ffff5e7cc35af000 | x8 : 0000000000000001 x7 : 3d4d455453595342 x6 : 000000004e514553 | x5 : ffff1f6501499265 x4 : ffff1f650ff60b10 x3 : 0000000000000620 | x2 : ffff80008002ba78 x1 : 0000000000000000 x0 : 0000000000000000 | Call trace: | cancel_delayed_work+0x34/0x44 | deferred_probe_extend_timeout+0x20/0x70 | driver_register+0xa8/0x110 | __platform_driver_register+0x28/0x3c | syscon_init+0x24/0x38 | do_one_initcall+0xe4/0x338 | do_initcall_level+0xac/0x178 | do_initcalls+0x5c/0xa0 | do_basic_setup+0x20/0x30 | kernel_init_freeable+0x8c/0xf8 | kernel_init+0x28/0x1b4 | ret_from_fork+0x10/0x20 | Code: f9000fbf 97fffa2f 39400268 37100048 (d42aa2a0) | ---[end trace 0000000000000000]--- | Kernel panic - not syncing: UBSAN: integer subtraction overflow: Fatal exception This is due to shift_and_mask() using a signed immediate to construct the mask and being called with a shift of 31 (WORK_OFFQ_POOL_SHIFT) so that it ends up decrementing from INT_MIN. Use an unsigned constant '1U' to generate the mask in shift_and_mask().	5.5	More Details
CVE-2024-44982	In the Linux kernel, the following vulnerability has been resolved: drm/msm/dpu: cleanup FB if dpu_format_populate_layout fails If the dpu_format_populate_layout() fails, then FB is prepared, but not cleaned up. This ends up leaking the pin_count on the GEM object and causes a splat during DRM file closure: msm_obj->pin_count WARNING: CPU: 2 PID: 569 at drivers/gpu/drm/msm/msm_gem.c:121 update_lru_locked+0xc4/0xcc [...] Call trace: update_lru_locked+0xc4/0xcc put_pages+0xac/0x100 msm_gem_free_object+0x138/0x180 drm_gem_object_free+0x1c/0x30 drm_gem_object_handle_put_unlocked+0x108/0x10c drm_gem_object_release_handle+0x58/0x70 idr_for_each+0x68/0xec drm_gem_release+0x28/0x40 drm_file_free+0x174/0x234 drm_release+0xb0/0x160 __fput+0xc0/0x2c8 __fput_sync+0x50/0x5c __arm64_sys_close+0x38/0x7c invoke_syscall+0x48/0x118 el0_svc_common.constprop.0+0x40/0xe0 do_el0_svc+0x1c/0x28 el0_svc+0x4c/0x120 el0t_64_sync_handler+0x100/0x12c el0t_64_sync+0x190/0x194 irq event stamp: 129818 hardirqs last enabled at (129817): [<ffffa5f6d953fcc0>] console_unlock+0x118/0x124 hardirqs last disabled at (129818): [<ffffa5f6da7dcf04>] el1_dbg+0x24/0x8c softirqs last enabled at (129808): [<ffffa5f6d94afc18>] handle_softirqs+0x4c8/0x4e8 softirqs last disabled at (129785): [<ffffa5f6d94105e4>] __do_softirq+0x14/0x20 Patchwork: https://patchwork.freedesktop.org/patch/600714/	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44984	In the Linux kernel, the following vulnerability has been resolved: bnxt_en: Fix double DMA unmapping for XDP_REDIRECT Remove the dma_unmap_page_attrs() call in the driver's XDP_REDIRECT code path. This should have been removed when we let the page pool handle the DMA mapping. This bug causes the warning: WARNING: CPU: 7 PID: 59 at drivers/iommu/dma-iommu.c:1198 iommu_dma_unmap_page+0xd5/0x100 CPU: 7 PID: 59 Comm: ksoftirqd/7 Tainted: G W 6.8.0-1010-gcp #11-Ubuntu Hardware name: Dell Inc. PowerEdge R7525/0PYVT1, BIOS 2.15.2 04/02/2024 RIP: 0010:iommu_dma_unmap_page+0xd5/0x100 Code: 89 ee 48 89 df e8 cb f2 69 ff 48 83 c4 08 5b 41 5c 41 5d 41 5e 41 5f 5d 31 c0 31 d2 31 c9 31 f6 31 ff 45 31 c0 e9 ab 17 71 00 <0f> 0b 48 83 c4 08 5b 41 5c 41 5d 41 5e 41 5f 5d 31 c0 31 d2 31 c9 RSP: 0018:ffffab1fc0597a48 EFLAGS: 00010246 RAX: 0000000000000000 RBX: ffff99ff838280c8 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffffab1fc0597a78 R08: 0000000000000002 R09: ffffab1fc0597c1c R10: ffffab1fc0597cd3 R11: ffff99ffe375acd8 R12: 00000000e65b9000 R13: 0000000000000050 R14: 0000000000001000 R15: 0000000000000002 FS: 0000000000000000(0000) GS:ffff9a06efb80000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000565c34c37210 CR3: 00000005c7e3e000 CR4: 0000000000350ef0 ? show_regs+0x6d/0x80 ? __warn+0x89/0x150 ? iommu_dma_unmap_page+0xd5/0x100 ? report_bug+0x16a/0x190 ? handle_bug+0x51/0xa0 ? exc_invalid_op+0x18/0x80 ? iommu_dma_unmap_page+0xd5/0x100 ? iommu_dma_unmap_page+0x35/0x100 dma_unmap_page_attrs+0x55/0x220 ? bpf_prog_4d7e87c0d30db711_xdp_dispatcher+0x64/0x9f bnxt_rx_xdp+0x237/0x520 [bnxt_en] bnxt_rx_pkt+0x640/0xdd0 [bnxt_en] __bnxt_poll_work+0x1a1/0x3d0 [bnxt_en] bnxt_poll+0xaa/0x1e0 [bnxt_en] __napi_poll+0x33/0x1e0 net_rx_action+0x18a/0x2f0	5.5	More Details
CVE-2024-44988	In the Linux kernel, the following vulnerability has been resolved: net: dsa: mv88e6xxx: Fix out-of-bound access If an ATU violation was caused by a CPU Load operation, the SPID could be larger than DSA_MAX_PORTS (the size of mv88e6xxx_chip.ports[] array).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44989	In the Linux kernel, the following vulnerability has been resolved: bonding: fix xfrm real_dev null pointer dereference We shouldn't set real_dev to NULL because packets can be in transit and xfrm might call xdo_dev_offload_ok() in parallel. All callbacks assume real_dev is set. Example trace: kernel: BUG: unable to handle page fault for address: 0000000000001030 kernel: bond0: (slave eni0np1): making interface the new active one kernel: #PF: supervisor write access in kernel mode kernel: #PF: error_code(0x0002) - not-present page kernel: PGD 0 P4D 0 kernel: Oops: 0002 [#1] PREEMPT SMP kernel: CPU: 4 PID: 2237 Comm: ping Not tainted 6.7.7+ #12 kernel: Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-2.fc40 04/01/2014 kernel: RIP: 0010:nsim_ipsec_offload_ok+0xc/0x20 [netdevsim] kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: Code: e0 0f 0b 48 83 7f 38 00 74 de 0f 0b 48 8b 47 08 48 8b 37 48 8b 78 40 e9 b2 e5 9a d7 66 90 0f 1f 44 00 00 48 8b 86 80 02 00 00 <83> 80 30 10 00 00 01 b8 01 00 00 00 c3 0f 1f 80 00 00 00 00 0f 1f kernel: bond0: (slave eni0np1): making interface the new active one kernel: RSP: 0018:ffffabde81553b98 EFLAGS: 00010246 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: kernel: RAX: 0000000000000000 RBX: ffff9eb404e74900 RCX: ffff9eb403d97c60 kernel: RDX: ffffffffc090de10 RSI: ffff9eb404e74900 RDI: ffff9eb3c5de9e00 kernel: RBP: ffff9eb3c0a42000 R08: 0000000000000010 R09: 0000000000000014 kernel: R10: 7974203030303030 R11: 3030303030303030 R12: 0000000000000000 kernel: R13: ffff9eb3c5de9e00 R14: ffffabde81553cc8 R15: ffff9eb404c53000 kernel: FS: 00007f2a77a3ad00(0000) GS:ffff9eb43bd00000(0000) knlGS:0000000000000000 kernel: CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 kernel: CR2: 0000000000001030 CR3: 00000001122ab000 CR4: 0000000000350ef0 kernel: bond0: (slave eni0np1): making interface the new active one kernel: Call Trace: kernel: <TASK> kernel: ? __die+0x1f/0x60 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: ? page_fault_oops+0x142/0x4c0 kernel: ? do_user_addr_fault+0x65/0x670 kernel: ? kvm_read_and_reset_apf_flags+0x3b/0x50 kernel: bond0: (slave eni0np1): making interface the new active one kernel: ? exc_page_fault+0x7b/0x180 kernel: ? asm_exc_page_fault+0x22/0x30 kernel: ? nsim_bpf_uninit+0x50/0x50 [netdevsim] kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: ? nsim_ipsec_offload_ok+0xc/0x20 [netdevsim] kernel: bond0: (slave eni0np1): making interface the new active one kernel: bond_ipsec_offload_ok+0x7b/0x90 [bonding] kernel: xfrm_output+0x61/0x3b0 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: ip_push_pending_frames+0x56/0x80	5.5	More Details
CVE-2024-44990	In the Linux kernel, the following vulnerability has been resolved: bonding: fix null pointer deref in bond_ipsec_offload_ok We must check if there is an active slave before dereferencing the pointer.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44991	In the Linux kernel, the following vulnerability has been resolved: tcp: prevent concurrent execution of tcp_sk_exit_batch Its possible that two threads call tcp_sk_exit_batch() concurrently, once from the cleanup_net workqueue, once from a task that failed to clone a new netns. In the latter case, error unwinding calls the exit handlers in reverse order for the 'failed' netns. tcp_sk_exit_batch() calls tcp_twsk_purge(). Problem is that since commit b099ce2602d8 ("net: Batch inet_twsk_purge"), this function picks up twsk in any dying netns, not just the one passed in via exit_batch list. This means that the error unwind of setup_net() can "steal" and destroy timewait sockets belonging to the exiting netns. This allows the netns exit worker to proceed to call WARN_ON_ONCE(!refcount_dec_and_test(&net->ipv4.tcp_death_row.tw_refcount)); without the expected 1 -> 0 transition, which then splats. At same time, error unwind path that is also running inet_twsk_purge() will splat as well: WARNING: .. at lib/refcount.c:31 refcount_warn_saturate+0x1ed/0x210 ... refcount_dec include/linux/refcount.h:351 [inline] inet_twsk_kill+0x758/0x9c0 net/ipv4/inet_timewait_sock.c:70 inet_twsk_deschedule_put net/ipv4/inet_timewait_sock.c:221 inet_twsk_purge+0x725/0x890 net/ipv4/inet_timewait_sock.c:304 tcp_sk_exit_batch+0x1c/0x170 net/ipv4/tcp_ipv4.c:3522 ops_exit_list+0x128/0x180 net/core/net_namespace.c:178 setup_net+0x714/0xb40 net/core/net_namespace.c:375 copy_net_ns+0x2f0/0x670 net/core/net_namespace.c:508 create_new_namespaces+0x3ea/0xb10 kernel/nsproxy.c:110 ... because refcount_dec() of tw_refcount unexpectedly dropped to 0. This doesn't seem like an actual bug (no tw sockets got lost and I don't see a use-after-free) but as erroneous trigger of debug check. Add a mutex to force strict ordering: the task that calls tcp_twsk_purge() blocks other task from doing final _dec_and_test before mutex-owner has removed all tw sockets of dying netns.	5.5	More Details
CVE-2024-44992	In the Linux kernel, the following vulnerability has been resolved: smb/client: avoid possible NULL dereference in cifs_free_subrequest() Clang static checker (scan-build) warning: cifsglob.h:line 890, column 3 Access to field 'ops' results in a dereference of a null pointer. Commit 519be989717c ("cifs: Add a tracepoint to track credits involved in R/W requests") adds a check for 'rdata->server', and let clang throw this warning about NULL dereference. When 'rdata->credits.value != 0 && rdata->server == NULL' happens, add_credits_and_wake_if() will call rdata->server->ops->add_credits(). This will cause NULL dereference problem. Add a check for 'rdata->server' to avoid NULL dereference.	5.5	More Details
CVE-2024-45107	Acrobat Reader versions 20.005.30636, 24.002.20964, 24.001.30123, 24.002.20991 and earlier are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-44994	In the Linux kernel, the following vulnerability has been resolved: iommu: Restore lost return in iommu_report_device_fault() When iommu_report_device_fault gets called with a partial fault it is supposed to collect the fault into the group and then return. Instead the return was accidently deleted which results in trying to process the fault and an eventual crash. Deleting the return was a typo, put it back.	5.5	More Details
CVE-2024-20503	A vulnerability in Cisco Duo Epic for Hyperdrive could allow an authenticated, local attacker to view sensitive information in cleartext on an affected system. This vulnerability is due to improper storage of an unencrypted registry key. A low-privileged attacker could exploit this vulnerability by viewing or querying the registry key on the affected system. A successful exploit could allow the attacker to view sensitive information in cleartext.	5.5	More Details
CVE-2024-44995	In the Linux kernel, the following vulnerability has been resolved: net: hns3: fix a deadlock problem when config TC during resetting When config TC during the reset process, may cause a deadlock, the flow is as below: pf reset start ｜ ▼ ...... setup tc ｜ ｜ ▼ ▼ DOWN: napi_disable() napi_disable() (skip) ｜ ｜ ｜ ▼ ▼ .... ｜ ｜ ▼ ｜ napi_enable() ｜ ▼ UINIT: netif_napi_del() ｜ ▼ ...... ｜ ▼ INIT: netif_napi_add() ｜ ▼ ...... global reset start ｜ ｜ ▼ ▼ UP: napi_enable()(skip) ...... ｜ ｜ ▼ ▼ ...... napi_disable() In reset process, the driver will DOWN the port and then UINIT, in this case, the setup tc process will UP the port before UINIT, so cause the problem. Adds a DOWN process in UINIT to fix it.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44996	In the Linux kernel, the following vulnerability has been resolved: vsock: fix recursive ->recvmsg calls After a vsock socket has been added to a BPF sockmap, its prot->recvmsg has been replaced with vsock_bpf_recvmsg(). Thus the following recursiion could happen: vsock_bpf_recvmsg() -> __vsock_recvmsg() -> vsock_connectible_recvmsg() -> prot->recvmsg() -> vsock_bpf_recvmsg() again We need to fix it by calling the original ->recvmsg() without any BPF sockmap logic in __vsock_recvmsg().	5.5	More Details
CVE-2024-45000	In the Linux kernel, the following vulnerability has been resolved: fs/netfs/fscache_cookie: add missing "n_accesses" check This fixes a NULL pointer dereference bug due to a data race which looks like this: BUG: kernel NULL pointer dereference, address: 0000000000000008 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] SMP PTI CPU: 33 PID: 16573 Comm: kworker/u97:799 Not tainted 6.8.7-cm4all1-hp+ #43 Hardware name: HP ProLiant DL380 Gen9/ProLiant DL380 Gen9, BIOS P89 10/17/2018 Workqueue: events_unbound netfs_rreq_write_to_cache_work RIP: 0010:cachefiles_prepare_write+0x30/0xa0 Code: 57 41 56 45 89 ce 41 55 49 89 cd 41 54 49 89 d4 55 53 48 89 fb 48 83 ec 08 48 8b 47 08 48 83 7f 10 00 48 89 34 24 48 8b 68 20 <48> 8b 45 08 4c 8b 38 74 45 49 8b 7f 50 e8 4e a9 b0 ff 48 8b 73 10 RSP: 0018:ffffb4e78113bde0 EFLAGS: 00010286 RAX: ffff976126be6d10 RBX: ffff97615cdb8438 RCX: 0000000000020000 RDX: ffff97605e6c4c68 RSI: ffff97605e6c4c60 RDI: ffff97615cdb8438 RBP: 0000000000000000 R08: 0000000000278333 R09: 0000000000000001 R10: ffff97605e6c4600 R11: 0000000000000001 R12: ffff97605e6c4c68 R13: 0000000000020000 R14: 0000000000000001 R15: ffff976064fe2c00 FS: 0000000000000000(0000) GS:ffff9776dfd40000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000008 CR3: 000000005942c002 CR4: 00000000001706f0 Call Trace: <TASK> ? __die+0x1f/0x70 ? page_fault_oops+0x15d/0x440 ? search_module_extables+0xe/0x40 ? fixup_exception+0x22/0x2f0 ? exc_page_fault+0x5f/0x100 ? asm_exc_page_fault+0x22/0x30 ? cachefiles_prepare_write+0x30/0xa0 netfs_rreq_write_to_cache_work+0x135/0x2e0 process_one_work+0x137/0x2c0 worker_thread+0x2e9/0x400 ? __pfx_worker_thread+0x10/0x10 kthread+0xcc/0x100 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x30/0x50 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1b/0x30 </TASK> Modules linked in: CR2: 0000000000000008 ---[end trace 0000000000000000]--- This happened because fscache_cookie_state_machine() was slow and was still running while another process invoked fscache_unuse_cookie(); this led to a fscache_cookie_lru_do_one() call, setting the FSCACHE_COOKIE_DO_LRU_DISCARD flag, which was picked up by fscache_cookie_state_machine(), withdrawing the cookie via cachefiles_withdraw_cookie(), clearing cookie->cache_priv. At the same time, yet another process invoked cachefiles_prepare_write(), which found a NULL pointer in this code line: struct cachefiles_object *object = cachefiles_cres_object(cres); The next line crashes, obviously: struct cachefiles_cache *cache = object->volume->cache; During cachefiles_prepare_write(), the "n_accesses" counter is non-zero (via fscache_begin_operation()). The cookie must not be withdrawn until it drops to zero. The counter is checked by fscache_cookie_state_machine() before switching to FSCACHE_COOKIE_STATE_RELINQUISHING and FSCACHE_COOKIE_STATE_WITHDRAWING (in "case FSCACHE_COOKIE_STATE_FAILED"), but not for FSCACHE_COOKIE_STATE_LRU_DISCARDING ("case FSCACHE_COOKIE_STATE_ACTIVE"). This patch adds the missing check. With a non-zero access counter, the function returns and the next fscache_end_cookie_access() call will queue another fscache_cookie_state_machine() call to handle the still-pending FSCACHE_COOKIE_DO_LRU_DISCARD.	5.5	More Details
CVE-2024-38254	Windows Authentication Information Disclosure Vulnerability	5.5	More Details
CVE-2024-38256	Windows Kernel-Mode Driver Information Disclosure Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45001	In the Linux kernel, the following vulnerability has been resolved: net: mana: Fix RX buf alloc_size alignment and atomic op panic The MANA driver's RX buffer alloc_size is passed into napi_build_skb() to create SKB. skb_shinfo(skb) is located at the end of skb, and its alignment is affected by the alloc_size passed into napi_build_skb(). The size needs to be aligned properly for better performance and atomic operations. Otherwise, on ARM64 CPU, for certain MTU settings like 4000, atomic operations may panic on the skb_shinfo(skb)->dataref due to alignment fault. To fix this bug, add proper alignment to the alloc_size calculation. Sample panic info: [253.298819] Unable to handle kernel paging request at virtual address ffff000129ba5cce [253.300900] Mem abort info: [253.301760] ESR = 0x0000000096000021 [253.302825] EC = 0x25: DABT (current EL), IL = 32 bits [253.304268] SET = 0, FnV = 0 [253.305172] EA = 0, S1PTW = 0 [253.306103] FSC = 0x21: alignment fault Call trace: __skb_clone+0xfc/0x198 skb_clone+0x78/0xe0 raw6_local_deliver+0xfc/0x228 ip6_protocol_deliver_rcu+0x80/0x500 ip6_input_finish+0x48/0x80 ip6_input+0x48/0xc0 ip6_sublist_rcv_finish+0x50/0x78 ip6_sublist_rcv+0x1cc/0x2b8 ipv6_list_rcv+0x100/0x150 __netif_receive_skb_list_core+0x180/0x220 netif_receive_skb_list_internal+0x198/0x2a8 __napi_poll+0x138/0x250 net_rx_action+0x148/0x330 handle_softirqs+0x12c/0x3a0	5.5	More Details
CVE-2024-45006	In the Linux kernel, the following vulnerability has been resolved: xhci: Fix Panther point NULL pointer deref at full-speed re-enumeration re-enumerating full-speed devices after a failed address device command can trigger a NULL pointer dereference. Full-speed devices may need to reconfigure the endpoint 0 Max Packet Size value during enumeration. Usb core calls usb_ep0_reinit() in this case, which ends up calling xhci_configure_endpoint(). On Panther point xHC the xhci_configure_endpoint() function will additionally check and reserve bandwidth in software. Other hosts do this in hardware If xHC address device command fails then a new xhci_virt_device structure is allocated as part of re-enabling the slot, but the bandwidth table pointers are not set up properly here. This triggers the NULL pointer dereference the next time usb_ep0_reinit() is called and xhci_configure_endpoint() tries to check and reserve bandwidth [46710.713538] usb 3-1: new full-speed USB device number 5 using xhci_hcd [46710.713699] usb 3-1: Device not responding to setup address. [46710.917684] usb 3-1: Device not responding to setup address. [46711.125536] usb 3-1: device not accepting address 5, error -71 [46711.125594] BUG: kernel NULL pointer dereference, address: 0000000000000008 [46711.125600] #PF: supervisor read access in kernel mode [46711.125603] #PF: error_code(0x0000) - not-present page [46711.125606] PGD 0 P4D 0 [46711.125610] Oops: Oops: 0000 [#1] PREEMPT SMP PTI [46711.125615] CPU: 1 PID: 25760 Comm: kworker/1:2 Not tainted 6.10.3_2 #1 [46711.125620] Hardware name: Gigabyte Technology Co., Ltd. [46711.125623] Workqueue: usb_hub_wq hub_event [usbcore] [46711.125668] RIP: 0010:xhci_reserve_bandwidth (drivers/usb/host/xhci.c Fix this by making sure bandwidth table pointers are set up correctly after a failed address device command, and additionally by avoiding checking for bandwidth in cases like this where no actual endpoints are added or removed, i.e. only context for default control endpoint 0 is evaluated.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45005	In the Linux kernel, the following vulnerability has been resolved: KVM: s390: fix validity interception issue when gisa is switched off We might run into a SIE validity if gisa has been disabled either via using kernel parameter "kvm.use_gisa=0" or by setting the related sysfs attribute to N (echo N >/sys/module/kvm/parameters/use_gisa). The validity is caused by an invalid value in the SIE control block's gisa designation. That happens because we pass the uninitialized gisa origin to virt_to_phys() before writing it to the gisa designation. To fix this we return 0 in kvm_s390_get_gisa_desc() if the origin is 0. kvm_s390_get_gisa_desc() is used to determine which gisa designation to set in the SIE control block. A value of 0 in the gisa designation disables gisa usage. The issue surfaces in the host kernel with the following kernel message as soon a new kvm guest start is attemted. kvm: unhandled validity intercept 0x1011 WARNING: CPU: 0 PID: 781237 at arch/s390/kvm/intercept.c:101 kvm_handle_sie_intercept+0x42e/0x4d0 [kvm] Modules linked in: vhost_net tap tun xt_CHECKSUM xt_MASQUERADE xt_conntrack ipt_REJECT xt_tcpudp nft_compat x_tables nf_nat_tftp nf_conntrack_tftp vfio_pci_core irqbypass vhost_vsock vmw_vsock_virtio_transport_common vsock vhost vhost_iotlb kvm nft_fib_inet nft_fib_ipv4 nft_fib_ipv6 nft_fib nft_reject_inet nf_reject_ipv4 nf_reject_ipv6 nft_reject nft_ct nft_chain_nat nf_nat nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 ip_set nf_tables sunrpc mlx5_ib ib_uverbs ib_core mlx5_core uvdevice s390_trng eadm_sch vfio_ccw zcrypt_cex4 mdev vfio_iommu_type1 vfio sch_fq_codel drm i2c_core loop drm_panel_orientation_quirks configfs nfnetlink lcs ctcm fsm dm_service_time ghash_s390 prng chacha_s390 libchacha aes_s390 des_s390 libdes sha3_512_s390 sha3_256_s390 sha512_s390 sha256_s390 sha1_s390 sha_common dm_mirror dm_region_hash dm_log zfcp scsi_transport_fc scsi_dh_rdac scsi_dh_emc scsi_dh_alua pkey zcrypt dm_multipath rng_core autofs4 [last unloaded: vfio_pci] CPU: 0 PID: 781237 Comm: CPU 0/KVM Not tainted 6.10.0-08682-gcad9f11498ea #6 Hardware name: IBM 3931 A01 701 (LPAR) Krnl PSW : 0704c00180000000 000003d93deb0122 (kvm_handle_sie_intercept+0x432/0x4d0 [kvm]) R:0 T:1 IO:1 EX:1 Key:0 M:1 W:0 P:0 AS:3 CC:0 PM:0 RI:0 EA:3 Krnl GPRS: 000003d900000027 000003d900000023 0000000000000028 000002cd00000000 000002d063a00900 00000359c6daf708 00000000000bebb5 0000000000001eff 000002cfd82e9000 000002cfd80bc000 0000000000001011 000003d93deda412 000003ff8962df98 000003d93de77ce0 000003d93deb011e 00000359c6daf960 Krnl Code: 000003d93deb0112: c020fffe7259 larl %r2,000003d93de7e5c4 000003d93deb0118: c0e53fa8beac brasl %r14,000003d9bd3c7e70 #000003d93deb011e: af000000 mc 0,0 >000003d93deb0122: a728ffea lhi %r2,-22 000003d93deb0126: a7f4fe24 brc 15,000003d93deafd6e 000003d93deb012a: 9101f0b0 tm 176(%r15),1 000003d93deb012e: a774fe48 brc 7,000003d93deafdbe 000003d93deb0132: 40a0f0ae sth %r10,174(%r15) Call Trace: [<000003d93deb0122>] kvm_handle_sie_intercept+0x432/0x4d0 [kvm] ([<000003d93deb011e>] kvm_handle_sie_intercept+0x42e/0x4d0 [kvm]) [<000003d93deacc10>] vcpu_post_run+0x1d0/0x3b0 [kvm] [<000003d93deaceda>] __vcpu_run+0xea/0x2d0 [kvm] [<000003d93dead9da>] kvm_arch_vcpu_ioctl_run+0x16a/0x430 [kvm] [<000003d93de93ee0>] kvm_vcpu_ioctl+0x190/0x7c0 [kvm] [<000003d9bd728b4e>] vfs_ioctl+0x2e/0x70 [<000003d9bd72a092>] __s390x_sys_ioctl+0xc2/0xd0 [<000003d9be0e9222>] __do_syscall+0x1f2/0x2e0 [<000003d9be0f9a90>] system_call+0x70/0x98 Last Breaking-Event-Address: [<000003d9bd3c7f58>] __warn_printk+0xe8/0xf0	5.5	More Details
CVE-2024-45004	In the Linux kernel, the following vulnerability has been resolved: KEYS: trusted: dcp: fix leak of blob encryption key Trusted keys unseal the key blob on load, but keep the sealed payload in the blob field so that every subsequent read (export) will simply convert this field to hex and send it to userspace. With DCP-based trusted keys, we decrypt the blob encryption key (BEK) in the Kernel due hardware limitations and then decrypt the blob payload. BEK decryption is done in-place which means that the trusted key blob field is modified and it consequently holds the BEK in plain text. Every subsequent read of that key thus send the plain text BEK instead of the encrypted BEK to userspace. This issue only occurs when importing a trusted DCP-based key and then exporting it again. This should rarely happen as the common use cases are to either create a new trusted key and export it, or import a key blob and then just use it without exporting it again. Fix this by performing BEK decryption and encryption in a dedicated buffer. Further always wipe the plain text BEK buffer to prevent leaking the key via uninitialized memory.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44972	In the Linux kernel, the following vulnerability has been resolved: btrfs: do not clear page dirty inside extent_write_locked_range() [BUG] For subpage + zoned case, the following workload can lead to rsv data leak at unmount time: # mkfs.btrfs -f -s 4k $dev # mount $dev $mnt # fsstress -w -n 8 -d $mnt -s 1709539240 0/0: fiemap - no filename 0/1: copyrange read - no filename 0/2: write - no filename 0/3: rename - no source filename 0/4: creat f0 x:0 0 0 0/4: creat add id=0,parent=-1 0/5: writev f0[259 1 0 0 0 0] [778052,113,965] 0 0/6: ioctl(FIEMAP) f0[259 1 0 0 224 887097] [1294220,2291618343991484791,0x10000] -1 0/7: dwrite - xfsctl(XFS_IOC_DIOINFO) f0[259 1 0 0 224 887097] return 25, fallback to stat() 0/7: dwrite f0[259 1 0 0 224 887097] [696320,102400] 0 # umount $mnt The dmesg includes the following rsv leak detection warning (all call trace skipped): ------------[cut here]------------ WARNING: CPU: 2 PID: 4528 at fs/btrfs/inode.c:8653 btrfs_destroy_inode+0x1e0/0x200 [btrfs] ---[end trace 0000000000000000]--- ------------[cut here]------------ WARNING: CPU: 2 PID: 4528 at fs/btrfs/inode.c:8654 btrfs_destroy_inode+0x1a8/0x200 [btrfs] ---[end trace 0000000000000000]--- ------------[cut here]------------ WARNING: CPU: 2 PID: 4528 at fs/btrfs/inode.c:8660 btrfs_destroy_inode+0x1a0/0x200 [btrfs] ---[end trace 0000000000000000]--- BTRFS info (device sda): last unmount of filesystem 1b4abba9-de34-4f07-9e7f-157cf12a18d6 ------------[cut here]------------ WARNING: CPU: 3 PID: 4528 at fs/btrfs/block-group.c:4434 btrfs_free_block_groups+0x338/0x500 [btrfs] ---[end trace 0000000000000000]--- BTRFS info (device sda): space_info DATA has 268218368 free, is not full BTRFS info (device sda): space_info total=268435456, used=204800, pinned=0, reserved=0, may_use=12288, readonly=0 zone_unusable=0 BTRFS info (device sda): global_block_rsv: size 0 reserved 0 BTRFS info (device sda): trans_block_rsv: size 0 reserved 0 BTRFS info (device sda): chunk_block_rsv: size 0 reserved 0 BTRFS info (device sda): delayed_block_rsv: size 0 reserved 0 BTRFS info (device sda): delayed_refs_rsv: size 0 reserved 0 ------------[cut here]------------ WARNING: CPU: 3 PID: 4528 at fs/btrfs/block-group.c:4434 btrfs_free_block_groups+0x338/0x500 [btrfs] ---[end trace 0000000000000000]--- BTRFS info (device sda): space_info METADATA has 267796480 free, is not full BTRFS info (device sda): space_info total=268435456, used=131072, pinned=0, reserved=0, may_use=262144, readonly=0 zone_unusable=245760 BTRFS info (device sda): global_block_rsv: size 0 reserved 0 BTRFS info (device sda): trans_block_rsv: size 0 reserved 0 BTRFS info (device sda): chunk_block_rsv: size 0 reserved 0 BTRFS info (device sda): delayed_block_rsv: size 0 reserved 0 BTRFS info (device sda): delayed_refs_rsv: size 0 reserved 0 Above $dev is a tcmu-runner emulated zoned HDD, which has a max zone append size of 64K, and the system has 64K page size. [CAUSE] I have added several trace_printk() to show the events (header skipped): > btrfs_dirty_pages: r/i=5/259 dirty start=774144 len=114688 > btrfs_dirty_pages: r/i=5/259 dirty part of page=720896 off_in_page=53248 len_in_page=12288 > btrfs_dirty_pages: r/i=5/259 dirty part of page=786432 off_in_page=0 len_in_page=65536 > btrfs_dirty_pages: r/i=5/259 dirty part of page=851968 off_in_page=0 len_in_page=36864 The above lines show our buffered write has dirtied 3 pages of inode 259 of root 5: 704K 768K 832K 896K I l////l/////////////////l///////////l I 756K 868K l///l is the dirtied range using subpage bitmaps. and 'I' is the page boundary. Meanwhile all three pages (704K, 768K, 832K) have their PageDirty flag set. > btrfs_direct_write: r/i=5/259 start dio filepos=696320 len=102400 Then direct IO writ ---truncated---	5.5	More Details
CVE-2024-44973	In the Linux kernel, the following vulnerability has been resolved: mm, slub: do not call do_slab_free for kfence object In 782f8906f805 the freeing of kfence objects was moved from deep inside do_slab_free to the wrapper functions outside. This is a nice change, but unfortunately it missed one spot in __kmem_cache_free_bulk. This results in a crash like this: BUG skbuff_head_cache (Tainted: G S B E): Padding overwritten. 0xffff88907fea0f00-0xffff88907fea0fff @offset=3840 slab_err (mm/slub.c:1129) free_to_partial_list (mm/slub.c:? mm/slub.c:4036) slab_pad_check (mm/slub.c:864 mm/slub.c:1290) check_slab (mm/slub.c:?) free_to_partial_list (mm/slub.c:3171 mm/slub.c:4036) kmem_cache_alloc_bulk (mm/slub.c:? mm/slub.c:4495 mm/slub.c:4586 mm/slub.c:4635) napi_build_skb (net/core/skbuff.c:348 net/core/skbuff.c:527 net/core/skbuff.c:549) All the other callers to do_slab_free appear to be ok. Add a kfence_free check in __kmem_cache_free_bulk to avoid the crash.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44963	In the Linux kernel, the following vulnerability has been resolved: btrfs: do not BUG_ON() when freeing tree block after error When freeing a tree block, at btrfs_free_tree_block(), if we fail to create a delayed reference we don't deal with the error and just do a BUG_ON(). The error most likely to happen is -ENOMEM, and we have a comment mentioning that only -ENOMEM can happen, but that is not true, because in case qgroups are enabled any error returned from btrfs_qgroup_trace_extent_post() (can be -EUCLEAN or anything returned from btrfs_search_slot() for example) can be propagated back to btrfs_free_tree_block(). So stop doing a BUG_ON() and return the error to the callers and make them abort the transaction to prevent leaking space. Syzbot was triggering this, likely due to memory allocation failure injection.	5.5	More Details
CVE-2024-44968	In the Linux kernel, the following vulnerability has been resolved: tick/broadcast: Move per CPU pointer access into the atomic section The recent fix for making the take over of the broadcast timer more reliable retrieves a per CPU pointer in preemptible context. This went unnoticed as compilers hoist the access into the non-preemptible region where the pointer is actually used. But of course it's valid that the compiler keeps it at the place where the code puts it which rightfully triggers: BUG: using smp_processor_id() in preemptible [00000000] code: caller is hotplug_cpu__broadcast_tick_pull+0x1c/0xc0 Move it to the actual usage site which is in a non-preemptible region.	5.5	More Details
CVE-2024-44957	In the Linux kernel, the following vulnerability has been resolved: xen: privcmd: Switch from mutex to spinlock for irqfds irqfd_wakeup() gets EPOLLHUP, when it is called by eventfd_release() by way of wake_up_poll(&ctx->wqh, EPOLLHUP), which gets called under spin_lock_irqsave(). We can't use a mutex here as it will lead to a deadlock. Fix it by switching over to a spin lock.	5.5	More Details
CVE-2024-21753	A improper limitation of a pathname to a restricted directory ('path traversal') in Fortinet FortiClientEMS versions 7.2.0 through 7.2.4, 7.0.0 through 7.0.13, 6.4.0 through 6.4.9, 6.2.0 through 6.2.9, 6.0.0 through 6.0.8, 1.2.1 through 1.2.5 allows attacker to perform a denial of service, read or write a limited number of files via specially crafted HTTP requests	5.5	More Details
CVE-2024-44958	In the Linux kernel, the following vulnerability has been resolved: sched/smt: Fix unbalance sched_smt_present dec/inc I got the following warn report while doing stress test: jump label: negative count! WARNING: CPU: 3 PID: 38 at kernel/jump_label.c:263 static_key_slow_try_dec+0x9d/0xb0 Call Trace: <TASK> __static_key_slow_dec_cpuslocked+0x16/0x70 sched_cpu_deactivate+0x26e/0x2a0 cpuhp_invoke_callback+0x3ad/0x10d0 cpuhp_thread_fun+0x3f5/0x680 smpboot_thread_fn+0x56d/0x8d0 kthread+0x309/0x400 ret_from_fork+0x41/0x70 ret_from_fork_asm+0x1b/0x30 </TASK> Because when cpuset_cpu_inactive() fails in sched_cpu_deactivate(), the cpu offline failed, but sched_smt_present is decremented before calling sched_cpu_deactivate(), it leads to unbalanced dec/inc, so fix it by incrementing sched_smt_present in the error path.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44959	In the Linux kernel, the following vulnerability has been resolved: tracefs: Use generic inode RCU for synchronizing freeing With structure layout randomization enabled for 'struct inode' we need to avoid overlapping any of the RCU-used / initialized-only-once members, e.g. i_lru or i_sb_list to not corrupt related list traversals when making use of the rcu_head. For an unlucky structure layout of 'struct inode' we may end up with the following splat when running the ftrace selftests: [<...>] list_del corruption, ffff888103ee2cb0->next (tracefs_inode_cache+0x0/0x4e0 [slab object]) is NULL (prev is tracefs_inode_cache+0x78/0x4e0 [slab object]) [<...>] ------------[cut here]------------ [<...>] kernel BUG at lib/list_debug.c:54! [<...>] invalid opcode: 0000 [#1] PREEMPT SMP KASAN [<...>] CPU: 3 PID: 2550 Comm: mount Tainted: G N 6.8.12-grsec+ #122 ed2f536ca62f28b087b90e3cc906a8d25b3ddc65 [<...>] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.14.0-2 04/01/2014 [<...>] RIP: 0010:[<ffffffff84656018>] __list_del_entry_valid_or_report+0x138/0x3e0 [<...>] Code: 48 b8 99 fb 65 f2 ff ff ff ff e9 03 5c d9 fc cc 48 b8 99 fb 65 f2 ff ff ff ff e9 33 5a d9 fc cc 48 b8 99 fb 65 f2 ff ff ff ff <0f> 0b 4c 89 e9 48 89 ea 48 89 ee 48 c7 c7 60 8f dd 89 31 c0 e8 2f [<...>] RSP: 0018:fffffe80416afaf0 EFLAGS: 00010283 [<...>] RAX: 0000000000000098 RBX: ffff888103ee2cb0 RCX: 0000000000000000 [<...>] RDX: ffffffff84655fe8 RSI: ffffffff89dd8b60 RDI: 0000000000000001 [<...>] RBP: ffff888103ee2cb0 R08: 0000000000000001 R09: fffffbd0082d5f25 [<...>] R10: fffffe80416af92f R11: 0000000000000001 R12: fdf99c16731d9b6d [<...>] R13: 0000000000000000 R14: ffff88819ad4b8b8 R15: 0000000000000000 [<...>] RBX: tracefs_inode_cache+0x0/0x4e0 [slab object] [<...>] RDX: __list_del_entry_valid_or_report+0x108/0x3e0 [<...>] RSI: __func__.47+0x4340/0x4400 [<...>] RBP: tracefs_inode_cache+0x0/0x4e0 [slab object] [<...>] RSP: process kstack fffffe80416afaf0+0x7af0/0x8000 [mount 2550 2550] [<...>] R09: kasan shadow of process kstack fffffe80416af928+0x7928/0x8000 [mount 2550 2550] [<...>] R10: process kstack fffffe80416af92f+0x792f/0x8000 [mount 2550 2550] [<...>] R14: tracefs_inode_cache+0x78/0x4e0 [slab object] [<...>] FS: 00006dcb380c1840(0000) GS:ffff8881e0600000(0000) knlGS:0000000000000000 [<...>] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [<...>] CR2: 000076ab72b30e84 CR3: 000000000b088004 CR4: 0000000000360ef0 shadow CR4: 0000000000360ef0 [<...>] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [<...>] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [<...>] ASID: 0003 [<...>] Stack: [<...>] ffffffff818a2315 00000000f5c856ee ffffffff896f1840 ffff888103ee2cb0 [<...>] ffff88812b6b9750 0000000079d714b6 fffffbfff1e9280b ffffffff8f49405f [<...>] 0000000000000001 0000000000000000 ffff888104457280 ffffffff8248b392 [<...>] Call Trace: [<...>] <TASK> [<...>] [<ffffffff818a2315>] ? lock_release+0x175/0x380 fffffe80416afaf0 [<...>] [<ffffffff8248b392>] list_lru_del+0x152/0x740 fffffe80416afb48 [<...>] [<ffffffff8248ba93>] list_lru_del_obj+0x113/0x280 fffffe80416afb88 [<...>] [<ffffffff8940fd19>] ? _atomic_dec_and_lock+0x119/0x200 fffffe80416afb90 [<...>] [<ffffffff8295b244>] iput_final+0x1c4/0x9a0 fffffe80416afbb8 [<...>] [<ffffffff8293a52b>] dentry_unlink_inode+0x44b/0xaa0 fffffe80416afbf8 [<...>] [<ffffffff8293fefc>] __dentry_kill+0x23c/0xf00 fffffe80416afc40 [<...>] [<ffffffff8953a85f>] ? __this_cpu_preempt_check+0x1f/0xa0 fffffe80416afc48 [<...>] [<ffffffff82949ce5>] ? shrink_dentry_list+0x1c5/0x760 fffffe80416afc70 [<...>] [<ffffffff82949b71>] ? shrink_dentry_list+0x51/0x760 fffffe80416afc78 [<...>] [<ffffffff82949da8>] shrink_dentry_list+0x288/0x760 fffffe80416afc80 [<...>] [<ffffffff8294ae75>] shrink_dcache_sb+0x155/0x420 fffffe80416afcc8 [<...>] [<ffffffff8953a7c3>] ? debug_smp_processor_id+0x23/0xa0 fffffe80416afce0 [<...>] [<ffffffff8294ad20>] ? do_one_tre ---truncated---	5.5	More Details
CVE-2024-44960	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: core: Check for unset descriptor Make sure the descriptor has been set before looking at maxpacket. This fixes a null pointer panic in this case. This may happen if the gadget doesn't properly set up the endpoint for the current speed, or the gadget descriptors are malformed and the descriptor for the speed/endpoint are not found. No current gadget driver is known to have this problem, but this may cause a hard-to-find bug during development of new gadgets.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44961	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Forward soft recovery errors to userspace As we discussed before[1], soft recovery should be forwarded to userspace, or we can get into a really bad state where apps will keep submitting hanging command buffers cascading us to a hard reset. 1: https://lore.kernel.org/all/bf23d5ed-9a6b-43e7-84ee-8cbfd0d60f18@froggi.es/ (cherry picked from commit 434967aadbbbe3ad9103cc29e9a327de20fdba01)	5.5	More Details
CVE-2024-44962	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btnxpuart: Shutdown timer and prevent rearming when driver unloading When unload the btnxpuart driver, its associated timer will be deleted. If the timer happens to be modified at this moment, it leads to the kernel call this timer even after the driver unloaded, resulting in kernel panic. Use timer_shutdown_sync() instead of del_timer_sync() to prevent rearming. panic log: Internal error: Oops: 0000000086000007 [#1] PREEMPT SMP Modules linked in: algif_hash algif_skcipher af_alg moal(O) mlan(O) crct10dif_ce polyval_ce polyval_generic snd_soc_imx_card snd_soc_fsl_asoc_card snd_soc_imx_audmux mxc_jpeg_encdec v4l2_jpeg snd_soc_wm8962 snd_soc_fsl_micfil snd_soc_fsl_sai flexcan snd_soc_fsl_utils ap130x rpmsg_ctrl imx_pcm_dma can_dev rpmsg_char pwm_fan fuse [last unloaded: btnxpuart] CPU: 5 PID: 723 Comm: memtester Tainted: G O 6.6.23-lts-next-06207-g4aef2658ac28 #1 Hardware name: NXP i.MX95 19X19 board (DT) pstate: 20400009 (nzCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : 0xffff80007a2cf464 lr : call_timer_fn.isra.0+0x24/0x80 ... Call trace: 0xffff80007a2cf464 __run_timers+0x234/0x280 run_timer_softirq+0x20/0x40 __do_softirq+0x100/0x26c ____do_softirq+0x10/0x1c call_on_irq_stack+0x24/0x4c do_softirq_own_stack+0x1c/0x2c irq_exit_rcu+0xc0/0xdc el0_interrupt+0x54/0xd8 __el0_irq_handler_common+0x18/0x24 el0t_64_irq_handler+0x10/0x1c el0t_64_irq+0x190/0x194 Code: ???????? ???????? ???????? ???????? (????????) ---[end trace 0000000000000000]--- Kernel panic - not syncing: Oops: Fatal exception in interrupt SMP: stopping secondary CPUs Kernel Offset: disabled CPU features: 0x0,c0000000,40028143,1000721b Memory Limit: none ---[end Kernel panic - not syncing: Oops: Fatal exception in interrupt]---	5.5	More Details
CVE-2024-44950	In the Linux kernel, the following vulnerability has been resolved: serial: sc16is7xx: fix invalid FIFO access with special register set When enabling access to the special register set, Receiver time-out and RHR interrupts can happen. In this case, the IRQ handler will try to read from the FIFO thru the RHR register at address 0x00, but address 0x00 is mapped to DLL register, resulting in erroneous FIFO reading. Call graph example: sc16is7xx_startup(): entry sc16is7xx_ms_proc(): entry sc16is7xx_set_termios(): entry sc16is7xx_set_baud(): DLH/DLL = $009C --> access special register set sc16is7xx_port_irq() entry --> IIR is 0x0C sc16is7xx_handle_rx() entry sc16is7xx_fifo_read(): --> unable to access FIFO (RHR) because it is mapped to DLL (LCR=LCR_CONF_MODE_A) sc16is7xx_set_baud(): exit --> Restore access to general register set Fix the problem by claiming the efr_lock mutex when accessing the Special register set.	5.5	More Details
CVE-2024-44965	In the Linux kernel, the following vulnerability has been resolved: x86/mm: Fix pti_clone_pgtable() alignment assumption Guenter reported dodgy crashes on an i386-nosmp build using GCC-11 that had the form of endless traps until entry stack exhaust and then #DF from the stack guard. It turned out that pti_clone_pgtable() had alignment assumptions on the start address, notably it hard assumes start is PMD aligned. This is true on x86_64, but very much not true on i386. These assumptions can cause the end condition to malfunction, leading to a 'short' clone. Guess what happens when the user mapping has a short copy of the entry text? Use the correct increment form for addr to avoid alignment assumptions.	5.5	More Details
CVE-2024-44966	In the Linux kernel, the following vulnerability has been resolved: binfmt_flat: Fix corruption when not offsetting data start Commit 04d82a6d0881 ("binfmt_flat: allow not offsetting data start") introduced a RISC-V specific variant of the FLAT format which does not allocate any space for the (obsolete) array of shared library pointers. However, it did not disable the code which initializes the array, resulting in the corruption of sizeof(long) bytes before the DATA segment, generally the end of the TEXT segment. Introduce MAX_SHARED_LIBS_UPDATE which depends on the state of CONFIG_BINFMT_FLAT_NO_DATA_START_OFFSET to guard the initialization of the shared library pointer region so that it will only be initialized if space is reserved for it.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40680	IBM MQ 9.3 CD and 9.4 LTS/CD could allow a local user to cause a denial of service due to improper memory allocation causing a segmentation fault.	5.5	More Details
CVE-2024-44970	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: SHAMPO, Fix invalid WQ linked list unlink When all the strides in a WQE have been consumed, the WQE is unlinked from the WQ linked list (mlx5_wq_ll_pop()). For SHAMPO, it is possible to receive CQEs with 0 consumed strides for the same WQE even after the WQE is fully consumed and unlinked. This triggers an additional unlink for the same wqe which corrupts the linked list. Fix this scenario by accepting 0 sized consumed strides without unlinking the WQE again.	5.5	More Details
CVE-2024-44969	In the Linux kernel, the following vulnerability has been resolved: s390/sclp: Prevent release of buffer in I/O When a task waiting for completion of a Store Data operation is interrupted, an attempt is made to halt this operation. If this attempt fails due to a hardware or firmware problem, there is a chance that the SCLP facility might store data into buffers referenced by the original operation at a later time. Handle this situation by not releasing the referenced data buffers if the halt attempt fails. For current use cases, this might result in a leak of few pages of memory in case of a rare hardware/firmware malfunction.	5.5	More Details
CVE-2024-44837	A cross-site scripting (XSS) vulnerability in the component \bean\Manager.java of Drug v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the user parameter.	5.4	More Details
CVE-2024-5309	The Form Vibes – Database Manager for Forms plugin for WordPress is vulnerable to unauthorized access of data and modification of data due to a missing capability check on the fv_export_csv, reset_settings, save_settings, save_columns_settings, get_analytics_data, get_event_logs_data, delete_submissions, and get_submissions functions in all versions up to, and including, 1.4.12. This makes it possible for authenticated attackers, with Subscriber-level access and above, to perform multiple unauthorized actions. NOTE: This vulnerability is partially fixed in version 1.4.12.	5.4	More Details
CVE-2024-38640	A cross-site scripting (XSS) vulnerability has been reported to affect Download Station. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following version: Download Station 5.8.6.283 (2024/06/21) and later	5.4	More Details
CVE-2024-6859	The WP MultiTasking WordPress plugin through 0.1.12 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	5.4	More Details
CVE-2024-44818	Cross Site Scripting vulnerability in ZZCMS v.2023 and before allows a remote attacker to obtain sensitive information via the HTTP_Referer header of the caina.php component.	5.4	More Details
CVE-2024-45177	An issue was discovered in za-internet C-MOR Video Surveillance 5.2401 and 6.00PL01. Due to improper input validation, the C-MOR web interface is vulnerable to persistent cross-site scripting (XSS) attacks. It was found out that the camera configuration is vulnerable to a persistent cross-site scripting attack due to insufficient user input validation.	5.4	More Details
CVE-2024-45285	The RFC enabled function module allows a low privileged user to perform denial of service on any user and also change or delete favourite nodes. By sending a crafted packet in the function module targeting specific parameters, the specific targeted user will no longer have access to any functionality of SAP GUI. There is low impact on integrity and availability of the application.	5.4	More Details
CVE-2024-42020	A Cross-site-scripting (XSS) vulnerability exists in the Reporter Widgets that allows HTML injection.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6282	The Master Addons – Free Widgets, Hover Effects, Toggle, Conditions, Animations for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the data-jltma-wrapper-link element in all versions up to, and including 2.0.6.4 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 clicks on the injected link.	5.4	More Details
CVE-2024-8121	The The Ultimate WordPress Toolkit – WP Extended plugin for WordPress is vulnerable to unauthorized modification of user names due to a missing capability check on the wpext_change_admin_name() function in all versions up to, and including, 3.0.8. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change an admin's username to a username of their liking as long as the default 'admin' was used.	5.4	More Details
CVE-2023-51368	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later	5.4	More Details
CVE-2024-8123	The The Ultimate WordPress Toolkit – WP Extended plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.0.8 via the duplicate_post function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Contributor-level access and above, to duplicate posts written by other authors including admins. This includes the ability to duplicate password-protected posts, which reveals their contents.	5.4	More Details
CVE-2024-44117	The RFC enabled function module allows a low privileged user to perform various actions, such as modifying the URLs of any user's favourite nodes and workbook ID. There is low impact on integrity and availability of the application.	5.4	More Details
CVE-2024-42371	The RFC enabled function module allows a low privileged user to delete the workplace favourites of any user. This vulnerability could be utilized to identify usernames and access information about targeted user's workplaces and nodes. There is low impact on integrity and availability of the application.	5.4	More Details
CVE-2023-51367	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later	5.4	More Details
CVE-2024-8413	Cross Site Scripting (XSS) vulnerability through the action parameter in index.php. Affected product codebase https://github.com/Bioshox/Raspcontrol and forks such as https://github.com/harmon25/raspcontrol . An attacker could exploit this vulnerability by sending a specially crafted JavaScript payload to an authenticated user and partially hijacking their session details. References list	5.4	More Details
CVE-2024-38217	Windows Mark of the Web Security Feature Bypass Vulnerability	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37991	A vulnerability has been identified in SIMATIC Reader RF610R CMIIT (6GT2811-6BC10-2AA0) (All versions < V4.2), SIMATIC Reader RF610R ETSI (6GT2811-6BC10-0AA0) (All versions < V4.2), SIMATIC Reader RF610R FCC (6GT2811-6BC10-1AA0) (All versions < V4.2), SIMATIC Reader RF615R CMIIT (6GT2811-6CC10-2AA0) (All versions < V4.2), SIMATIC Reader RF615R ETSI (6GT2811-6CC10-0AA0) (All versions < V4.2), SIMATIC Reader RF615R FCC (6GT2811-6CC10-1AA0) (All versions < V4.2), SIMATIC Reader RF650R ARIB (6GT2811-6AB20-4AA0) (All versions < V4.2), SIMATIC Reader RF650R CMIIT (6GT2811-6AB20-2AA0) (All versions < V4.2), SIMATIC Reader RF650R ETSI (6GT2811-6AB20-0AA0) (All versions < V4.2), SIMATIC Reader RF650R FCC (6GT2811-6AB20-1AA0) (All versions < V4.2), SIMATIC Reader RF680R ARIB (6GT2811-6AA10-4AA0) (All versions < V4.2), SIMATIC Reader RF680R CMIIT (6GT2811-6AA10-2AA0) (All versions < V4.2), SIMATIC Reader RF680R ETSI (6GT2811-6AA10-0AA0) (All versions < V4.2), SIMATIC Reader RF680R FCC (6GT2811-6AA10-1AA0) (All versions < V4.2), SIMATIC Reader RF685R ARIB (6GT2811-6CA10-4AA0) (All versions < V4.2), SIMATIC Reader RF685R CMIIT (6GT2811-6CA10-2AA0) (All versions < V4.2), SIMATIC Reader RF685R ETSI (6GT2811-6CA10-0AA0) (All versions < V4.2), SIMATIC Reader RF685R FCC (6GT2811-6CA10-1AA0) (All versions < V4.2), SIMATIC RF1140R (6GT2831-6CB00) (All versions < V1.1), SIMATIC RF1170R (6GT2831-6BB00) (All versions < V1.1), SIMATIC RF166C (6GT2002-0EE20) (All versions < V2.2), SIMATIC RF185C (6GT2002-0JE10) (All versions < V2.2), SIMATIC RF186C (6GT2002-0JE20) (All versions < V2.2), SIMATIC RF186CI (6GT2002-0JE50) (All versions < V2.2), SIMATIC RF188C (6GT2002-0JE40) (All versions < V2.2), SIMATIC RF188CI (6GT2002-0JE60) (All versions < V2.2), SIMATIC RF360R (6GT2801-5BA30) (All versions < V2.2). The service log files of the affected application can be accessed without proper authentication. This could allow an unauthenticated attacker to get access to sensitive information.	5.3	More Details
CVE-2024-8320	Missing authentication in Network Isolation of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to spoof Network Isolation status of managed devices.	5.3	More Details
CVE-2024-45591	XWiki Platform is a generic wiki platform. The REST API exposes the history of any page in XWiki of which the attacker knows the name. The exposed information includes for each modification of the page the time of the modification, the version number, the author of the modification (both username and displayed name) and the version comment. This information is exposed regardless of the rights setup, and even when the wiki is configured to be fully private. On a private wiki, this can be tested by accessing /xwiki/rest/wikis/xwiki/spaces/Main/pages/WebHome/history, if this shows the history of the main page then the installation is vulnerable. This has been patched in XWiki 15.10.9 and XWiki 16.3.0RC1.	5.3	More Details
CVE-2024-45412	Yeti bridges the gap between CTI and DFIR practitioners by providing a Forensics Intelligence platform and pipeline. Remote user-controlled data tags can reach a Unicode normalization with a compatibility form NFKD. Under Windows, such normalization is costly in resources and may lead to denial of service with attacks such as One Million Unicode payload. This can get worse with the use of special Unicode characters like U+2100 (℀), or U+2105 (℅) which could lead the payload size to be tripled. Versions prior to 2.1.11 are affected by this vulnerability. The patch is included in 2.1.11.	5.3	More Details
CVE-2024-8655	A vulnerability was found in Mercury MNVR816 up to 2.0.1.0.5. It has been classified as problematic. This affects an unknown part of the file /web-static/. The manipulation leads to files or directories accessible. 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.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49069	A vulnerability has been identified in Mendix Runtime V10 (All versions < V10.17.0 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 < V10.6.16 only if the basic authentication mechanism is used by the application), Mendix Runtime V8 (All versions < V8.18.33 only if the basic authentication mechanism is used by the application), Mendix Runtime V9 (All versions < V9.24.31 only if the basic authentication mechanism is used by the application). The authentication mechanism of affected applications contains an observable response discrepancy vulnerability when validating usernames. This could allow unauthenticated remote attackers to distinguish between valid and invalid usernames.	5.3	More Details
CVE-2024-7734	An unauthenticated remote attacker can exploit the behavior of the pathfinder TCP encapsulation service by establishing a high number of TCP connections to the pathfinder TCP encapsulation service. The impact is limited to blocking of valid IPsec VPN peers.	5.3	More Details
CVE-2024-8369	The EventPrime – Events Calendar, Bookings and Tickets plugin for WordPress is vulnerable to unauthorized access to Private or Password-protected events due to missing authorization checks in all versions up to, and including, 4.0.4.3. This makes it possible for unauthenticated attackers to view private or password-protected events.	5.3	More Details
CVE-2024-37993	A vulnerability has been identified in SIMATIC Reader RF610R CMIIT (6GT2811-6BC10-2AA0) (All versions < V4.2), SIMATIC Reader RF610R ETSI (6GT2811-6BC10-0AA0) (All versions < V4.2), SIMATIC Reader RF610R FCC (6GT2811-6BC10-1AA0) (All versions < V4.2), SIMATIC Reader RF615R CMIIT (6GT2811-6CC10-2AA0) (All versions < V4.2), SIMATIC Reader RF615R ETSI (6GT2811-6CC10-0AA0) (All versions < V4.2), SIMATIC Reader RF615R FCC (6GT2811-6CC10-1AA0) (All versions < V4.2), SIMATIC Reader RF650R ARIB (6GT2811-6AB20-4AA0) (All versions < V4.2), SIMATIC Reader RF650R CMIIT (6GT2811-6AB20-2AA0) (All versions < V4.2), SIMATIC Reader RF650R ETSI (6GT2811-6AB20-0AA0) (All versions < V4.2), SIMATIC Reader RF650R FCC (6GT2811-6AB20-1AA0) (All versions < V4.2), SIMATIC Reader RF680R ARIB (6GT2811-6AA10-4AA0) (All versions < V4.2), SIMATIC Reader RF680R CMIIT (6GT2811-6AA10-2AA0) (All versions < V4.2), SIMATIC Reader RF680R ETSI (6GT2811-6AA10-0AA0) (All versions < V4.2), SIMATIC Reader RF680R FCC (6GT2811-6AA10-1AA0) (All versions < V4.2), SIMATIC Reader RF685R ARIB (6GT2811-6CA10-4AA0) (All versions < V4.2), SIMATIC Reader RF685R CMIIT (6GT2811-6CA10-2AA0) (All versions < V4.2), SIMATIC Reader RF685R ETSI (6GT2811-6CA10-0AA0) (All versions < V4.2), SIMATIC Reader RF685R FCC (6GT2811-6CA10-1AA0) (All versions < V4.2), SIMATIC RF1140R (6GT2831-6CB00) (All versions < V1.1), SIMATIC RF1170R (6GT2831-6BB00) (All versions < V1.1), SIMATIC RF166C (6GT2002-0EE20) (All versions < V2.2), SIMATIC RF185C (6GT2002-0JE10) (All versions < V2.2), SIMATIC RF186C (6GT2002-0JE20) (All versions < V2.2), SIMATIC RF186CI (6GT2002-0JE50) (All versions < V2.2), SIMATIC RF188C (6GT2002-0JE40) (All versions < V2.2), SIMATIC RF188CI (6GT2002-0JE60) (All versions < V2.2), SIMATIC RF360R (6GT2801-5BA30) (All versions < V2.2). The affected applications do not authenticated the creation of Ajax2App instances. This could allow an unauthenticated attacker to cause a denial of service condition.	5.3	More Details
CVE-2024-45597	Pluto is a superset of Lua 5.4 with a focus on general-purpose programming. Scripts passing user-controlled values to http.request header values are affected. An attacker could use this to send arbitrary requests, potentially leveraging authentication tokens provided in the same headers table.	5.3	More Details
CVE-2023-30582	A vulnerability has been identified in Node.js version 20, affecting users of the experimental permission model when the --allow-fs-read flag is used with a non-* argument. This flaw arises from an inadequate permission model that fails to restrict file watching through the fs.watchFile API. As a result, malicious actors can monitor files that they do not have explicit read access to. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6010	The Cost Calculator Builder PRO plugin for WordPress is vulnerable to price manipulation in all versions up to, and including, 3.2.1. This is due to the plugin allowing the price field to be manipulated prior to processing via the 'create_cc_order' function, called from the Cost Calculator Builder plugin. This makes it possible for unauthenticated attackers to manipulate the price of orders submitted via the calculator. Note: this vulnerability was partially patched with the release of Cost Calculator Builder version 3.2.17.	5.3	More Details
CVE-2024-25584	Dovecot accepts dot LF DOT LF symbol as end of DATA command. RFC requires that it should always be CR LF DOT CR LF. This causes Dovecot to convert single mail with LF DOT LF in middle, into two emails when relaying to SMTP. Dovecot will split mail with LF DOT LF into two mails. Upgrade to latest released version. No publicly available exploits are known.	5.3	More Details
CVE-2023-39333	Maliciously crafted export names in an imported WebAssembly module can inject JavaScript code. The injected code may be able to access data and functions that the WebAssembly module itself does not have access to, similar to as if the WebAssembly module was a JavaScript module. This vulnerability affects users of any active release line of Node.js. The vulnerable feature is only available if Node.js is started with the `--experimental-wasm-modules` command line option.	5.3	More Details
CVE-2024-7415	The Remember Me Controls plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 2.0.1. This is due to the plugin allowing direct access to the bootstrap.php file which has display_errors on. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	5.3	More Details
CVE-2024-40865	The issue was addressed by suspending Persona when the virtual keyboard is active. This issue is fixed in visionOS 1.3. Inputs to the virtual keyboard may be inferred from Persona.	5.3	More Details
CVE-2024-38270	An insufficient entropy vulnerability caused by the improper use of a randomness function with low entropy for web authentication tokens generation exists in the Zyxel GS1900-10HP firmware version V2.80(AAZI.0)C0. This vulnerability could allow a LAN-based attacker a slight chance to gain a valid session token if multiple authenticated sessions are alive.	5.3	More Details
CVE-2024-8461	A vulnerability, which was classified as problematic, was found in D-Link DNS-320 2.02b01. This affects an unknown part of the file /cgi-bin/discovery.cgi of the component Web Management Interface. 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. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	5.3	More Details
CVE-2024-7381	The Geo Controller plugin for WordPress is vulnerable to unauthorized shortcode execution due to missing authorization and capability checks on the ajax__shortcode_cache function in all versions up to, and including, 8.6.9. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes available on the target site.	5.3	More Details
CVE-2022-4529	The Security, Antivirus, Firewall – S.A.F plugin for WordPress is vulnerable to IP Address Spoofing in versions up to, and including, 2.3.5. This is due to insufficient restrictions on where the IP Address information is being retrieved for request logging and login restrictions. Attackers can supply the X-Forwarded-For header with with a different IP Address that will be logged and can be used to bypass settings that may have blocked out an IP address from logging in.	5.3	More Details
CVE-2024-6835	The Ivory Search – WordPress Search Plugin plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 5.5.6 via the ajax_load_posts function. This makes it possible for unauthenticated attackers to extract text data from password-protected posts using the boolean-based attack on the AJAX search form	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6846	The Chatbot with ChatGPT WordPress plugin before 2.4.5 does not validate access on some REST routes, allowing for an unauthenticated user to purge error and chat logs	5.3	More Details
CVE-2024-7786	The Sensei LMS WordPress plugin before 4.24.2 does not properly protect some its REST API routes, allowing unauthenticated attackers to leak email templates.	5.3	More Details
CVE-2024-42343	Loway - CWE-204: Observable Response Discrepancy	5.3	More Details
CVE-2024-45052	Fides is an open-source privacy engineering platform. Prior to version 2.44.0, a timing-based username enumeration vulnerability exists in Fides Webserver authentication. This vulnerability allows an unauthenticated attacker to determine the existence of valid usernames by analyzing the time it takes for the server to respond to login requests. The discrepancy in response times between valid and invalid usernames can be leveraged to enumerate users on the system. This vulnerability enables a timing-based username enumeration attack. An attacker can systematically guess and verify which usernames are valid by measuring the server's response time to authentication requests. This information can be used to conduct further attacks on authentication such as password brute-forcing and credential stuffing. The vulnerability has been patched in Fides version `2.44.0`. Users are advised to upgrade to this version or later to secure their systems against this threat. There are no workarounds.	5.3	More Details
CVE-2024-44821	ZZCMS 2023 contains a vulnerability in the captcha reuse logic located in /inc/function.php. The checkyzm function does not properly refresh the captcha value after a failed validation attempt. As a result, an attacker can exploit this flaw by repeatedly submitting the same incorrect captcha response, allowing them to capture the correct captcha value through error messages.	5.3	More Details
CVE-2024-42424	Dell Precision Rack, 14G Intel BIOS versions prior to 2.22.2, contains an Improper Input Validation vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	5.3	More Details
CVE-2024-45449	Access permission verification vulnerability in the ringtone setting module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	5.1	More Details
CVE-2024-45442	Vulnerability of permission verification for APIs in the DownloadProviderMain module Impact: Successful exploitation of this vulnerability will affect availability.	5.1	More Details
CVE-2024-34641	Improper Export of Android Application Components in FeliCaTest prior to SMR Sep-2024 Release 1 allows local attackers to enable NFC configuration.	5.1	More Details
CVE-2024-34648	Improper Handling of Insufficient Permissions in KnoxMiscPolicy prior to SMR Sep-2024 Release 1 allows local attackers to access sensitive data.	5.1	More Details
CVE-2024-45157	An issue was discovered in Mbed TLS before 2.28.9 and 3.x before 3.6.1, in which the user-selected algorithm is not used. Unlike previously documented, enabling MBEDTLS_PSA_HMAC_DRBG_MD_TYPE does not cause the PSA subsystem to use HMAC_DRBG: it uses HMAC_DRBG only when MBEDTLS_PSA_CRYPTO_EXTERNAL_RNG and MBEDTLS_CTR_DRBG_C are disabled.	5.1	More Details
CVE-2024-8654	MongoDB Server may access non-initialized region of memory leading to unexpected behaviour when zero arguments are called in internal aggregation stage. This issue affected MongoDB Server v6.0 version 6.0.3.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44254	An authorization bypass through user-controlled key [CWE-639] vulnerability in FortiAnalyzer version 7.4.1 and before 7.2.5 and FortiManager version 7.4.1 and before 7.2.5 may allow a remote attacker with low privileges to read sensitive data via a crafted HTTP request.	5.0	More Details
CVE-2024-23184	Having a large number of address headers (From, To, Cc, Bcc, etc.) becomes excessively CPU intensive. With 100k header lines CPU usage is already 12 seconds, and in a production environment we observed 500k header lines taking 18 minutes to parse. Since this can be triggered by external actors sending emails to a victim, this is a security issue. An external attacker can send specially crafted messages that consume target system resources and cause outage. One can implement restrictions on address headers on MTA component preceding Dovecot. No publicly available exploits are known.	5.0	More Details
CVE-2024-43800	serve-static serves static files. serve-static passes untrusted user input - even after sanitizing it - to redirect() may execute untrusted code. This issue is patched in serve-static 1.16.0.	5.0	More Details
CVE-2024-43796	Express.js minimalist web framework for node. In express < 4.20.0, passing untrusted user input - even after sanitizing it - to response.redirect() may execute untrusted code. This issue is patched in express 4.20.0.	5.0	More Details
CVE-2024-43799	Send is a library for streaming files from the file system as a http response. Send passes untrusted user input to SendStream.redirect() which executes untrusted code. This issue is patched in send 0.19.0.	5.0	More Details
CVE-2024-37992	A vulnerability has been identified in SIMATIC Reader RF610R CMIIT (6GT2811-6BC10-2AA0) (All versions < V4.2), SIMATIC Reader RF610R ETSI (6GT2811-6BC10-0AA0) (All versions < V4.2), SIMATIC Reader RF610R FCC (6GT2811-6BC10-1AA0) (All versions < V4.2), SIMATIC Reader RF615R CMIIT (6GT2811-6CC10-2AA0) (All versions < V4.2), SIMATIC Reader RF615R ETSI (6GT2811-6CC10-0AA0) (All versions < V4.2), SIMATIC Reader RF615R FCC (6GT2811-6CC10-1AA0) (All versions < V4.2), SIMATIC Reader RF650R ARIB (6GT2811-6AB20-4AA0) (All versions < V4.2), SIMATIC Reader RF650R CMIIT (6GT2811-6AB20-2AA0) (All versions < V4.2), SIMATIC Reader RF650R ETSI (6GT2811-6AB20-0AA0) (All versions < V4.2), SIMATIC Reader RF650R FCC (6GT2811-6AB20-1AA0) (All versions < V4.2), SIMATIC Reader RF680R ARIB (6GT2811-6AA10-4AA0) (All versions < V4.2), SIMATIC Reader RF680R CMIIT (6GT2811-6AA10-2AA0) (All versions < V4.2), SIMATIC Reader RF680R ETSI (6GT2811-6AA10-0AA0) (All versions < V4.2), SIMATIC Reader RF680R FCC (6GT2811-6AA10-1AA0) (All versions < V4.2), SIMATIC Reader RF685R ARIB (6GT2811-6CA10-4AA0) (All versions < V4.2), SIMATIC Reader RF685R CMIIT (6GT2811-6CA10-2AA0) (All versions < V4.2), SIMATIC Reader RF685R ETSI (6GT2811-6CA10-0AA0) (All versions < V4.2), SIMATIC Reader RF685R FCC (6GT2811-6CA10-1AA0) (All versions < V4.2), SIMATIC RF1140R (6GT2831-6CB00) (All versions < V1.1), SIMATIC RF1170R (6GT2831-6BB00) (All versions < V1.1), SIMATIC RF166C (6GT2002-0EE20) (All versions < V2.2), SIMATIC RF185C (6GT2002-0JE10) (All versions < V2.2), SIMATIC RF186C (6GT2002-0JE20) (All versions < V2.2), SIMATIC RF186CI (6GT2002-0JE50) (All versions < V2.2), SIMATIC RF188C (6GT2002-0JE40) (All versions < V2.2), SIMATIC RF188CI (6GT2002-0JE60) (All versions < V2.2), SIMATIC RF360R (6GT2801-5BA30) (All versions < V2.2). The affected devices does not properly handle the error in case of exceeding characters while setting SNMP leading to the restart of the application.	4.9	More Details
CVE-2024-7918	The Pocket Widget WordPress plugin through 0.1.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2024-7955	The Starbox WordPress plugin before 3.5.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2024-44676	eladmin v2.7 and before is vulnerable to Cross Site Scripting (XSS) which allows an attacker to execute arbitrary code via LocalStoreController. java.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7891	The Floating Contact Button WordPress plugin before 2.8 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details
CVE-2024-6888	The Secure Copy Content Protection and Content Locking WordPress plugin before 4.1.7 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-45280	Due to insufficient encoding of user-controlled inputs, SAP NetWeaver AS Java allows malicious scripts to be executed in the login application. This has a limited impact on confidentiality and integrity of the application. There is no impact on availability.	4.8	More Details
CVE-2022-45856	An improper certificate validation vulnerability [CWE-295] in FortiClientWindows 6.4 all versions, 7.0.0 through 7.0.7, FortiClientMac 6.4 all versions, 7.0 all versions, 7.2.0 through 7.2.4, FortiClientLinux 6.4 all versions, 7.0 all versions, 7.2.0 through 7.2.4, FortiClientAndroid 6.4 all versions, 7.0 all versions, 7.2.0 and FortiClientiOS 5.6 all versions, 6.0.0 through 6.0.1, 7.0.0 through 7.0.6 SAML SSO feature may allow an unauthenticated attacker to man-in-the-middle the communication between the FortiClient and both the service provider and the identity provider.	4.8	More Details
CVE-2024-6722	The Chatbot Support AI: Free ChatGPT Chatbot, Woocommerce Chatbot WordPress plugin through 1.0.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-5561	The Popup Maker WordPress plugin before 1.19.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-6910	The EventON WordPress plugin before 2.2.17 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed.	4.8	More Details
CVE-2024-6889	The Secure Copy Content Protection and Content Locking WordPress plugin before 4.1.7 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2024-8372	Improper sanitization of the value of the '[srcset]' attribute in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing . This issue affects AngularJS versions 1.3.0-rc.4 and greater. Note: The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here https://docs.angularjs.org/misc/version-support-status .	4.8	More Details
CVE-2024-8373	Improper sanitization of the value of the [srcset] attribute in <source> HTML elements in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing . This issue affects all versions of AngularJS. Note: The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here https://docs.angularjs.org/misc/version-support-status .	4.8	More Details
CVE-2024-7318	A vulnerability was found in Keycloak. Expired OTP codes are still usable when using FreeOTP when the OTP token period is set to 30 seconds (default). Instead of expiring and deemed unusable around 30 seconds in, the tokens are valid for an additional 30 seconds totaling 1 minute. A one time passcode that is valid longer than its expiration time increases the attack window for malicious actors to abuse the system and compromise accounts. Additionally, it increases the attack surface because at any given time, two OTPs are valid.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44120	SAP NetWeaver Enterprise Portal is vulnerable to reflected cross site scripting due to insufficient encoding of user-controlled input. An unauthenticated attacker could craft a malicious URL and trick a user to click it. If the victim clicks on this crafted URL before it times out, then the attacker could read and manipulate user content in the browser.	4.7	More Details
CVE-2024-44954	In the Linux kernel, the following vulnerability has been resolved: ALSA: line6: Fix racy access to midibuf There can be concurrent accesses to line6 midibuf from both the URB completion callback and the rawmidi API access. This could be a cause of KMSAN warning triggered by syzkaller below (so put as reported-by here). This patch protects the midibuf call of the former code path with a spinlock for avoiding the possible races.	4.7	More Details
CVE-2024-21906	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later	4.7	More Details
CVE-2024-8559	A vulnerability, which was classified as critical, has been found in SourceCodester Online Food Menu 1.0. This issue affects some unknown processing of the file /endpoint/delete-menu.php. The manipulation of the argument menu leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2023-51712	An issue was discovered in Trusted Firmware-M through 2.0.0. The lack of argument verification in the logging subsystem allows attackers to read sensitive data via the login function.	4.7	More Details
CVE-2024-45003	In the Linux kernel, the following vulnerability has been resolved: vfs: Don't evict inode under the inode lru traversing context The inode reclaiming process(See function prune_icache_sb) collects all reclaimable inodes and mark them with I_FREEING flag at first, at that time, other processes will be stuck if they try getting these inodes (See function find_inode_fast), then the reclaiming process destroy the inodes by function dispose_list(). Some filesystems(eg. ext4 with ea_inode feature, ubifs with xattr) may do inode lookup in the inode evicting callback function, if the inode lookup is operated under the inode lru traversing context, deadlock problems may happen. Case 1: In function ext4_evict_inode(), the ea inode lookup could happen if ea_inode feature is enabled, the lookup process will be stuck under the evicting context like this: 1. File A has inode i_reg and an ea inode i_ea 2. getfattr(A, xattr_buf) // i_ea is added into lru // lru->i_ea 3. Then, following three processes running like this: PA PB echo 2 > /proc/sys/vm/drop_caches shrink_slab prune_dcache_sb // i_reg is added into lru, lru->i_ea->i_reg prune_icache_sb list_lru_walk_one inode_lru_isolate i_ea->i_state |= I_FREEING // set inode state inode_lru_isolate __iget(i_reg) spin_unlock(&i_reg->i_lock) spin_unlock(lru_lock) rm file A i_reg->nlink = 0 iput(i_reg) // i_reg->nlink is 0, do evict ext4_evict_inode ext4_xattr_delete_inode ext4_xattr_inode_dec_ref_all ext4_xattr_inode_iget ext4_iget(i_ea->i_ino) iget_locked find_inode_fast __wait_on_freeing_inode(i_ea) ----→ AA deadlock dispose_list // cannot be executed by prune_icache_sb wake_up_bit(&i_ea->i_state) Case 2: In deleted inode writing function ubifs_jnl_write_inode(), file deleting process holds BASEHD's wbuf->io_mutex while getting the xattr inode, which could race with inode reclaiming process(The reclaiming process could try locking BASEHD's wbuf->io_mutex in inode evicting function), then an ABBA deadlock problem would happen as following: 1. File A has inode ia and a xattr(with inode ixa), regular file B has inode ib and a xattr. 2. getfattr(A, xattr_buf) // ixa is added into lru // lru->ixa 3. Then, following three processes running like this: PA PB PC echo 2 > /proc/sys/vm/drop_caches shrink_slab prune_dcache_sb // ib and ia are added into lru, lru->ixa->ib->ia prune_icache_sb list_lru_walk_one inode_lru_isolate ixa->i_state |= I_FREEING // set inode state inode_lru_isolate __iget(ib) spin_unlock(&ib->i_lock) spin_unlock(lru_lock) rm file B ib->nlink = 0 rm file A iput(ia) ubifs_evict_inode(ia) ubifs_jnl_delete_inode(ia) ubifs_jnl_write_inode(ia) make_reservation(BASEHD) // Lock wbuf->io_mutex ubifs_iget(ixa->i_ino) iget_locked find_inode_fast __wait_on_freeing_inode(ixa) | iput(ib) // ib->nlink is 0, do evict | ubifs_evict_inode | ubifs_jnl_delete_inode(ib) ↓ ubifs_jnl_write_inode ABBA deadlock ←-----make_reservation(BASEHD) dispose_list // cannot be executed by prune_icache_sb wake_up_bit(&ixa->i_state) Fix the possible deadlock by using new inode state flag I_LRU_ISOLATING to pin the inode in memory while inode_lru_isolate(---truncated---	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8523	A vulnerability was found in lmxcms up to 1.4 and classified as critical. Affected by this issue is the function formatData of the file /admin.php?m=Acquisi&a=testcj&lid=1 of the component SQL Command Execution Module. The manipulation of the argument data leads to code injection. 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.	4.7	More Details
CVE-2024-41927	Cleartext transmission of sensitive information vulnerability exists in multiple IDEC PLCs. If an attacker sends a specific command to PLC's serial communication port, user credentials may be obtained. As a result, the program of the PLC may be obtained, and the PLC may be manipulated.	4.6	More Details
CVE-2024-44815	Vulnerability in Hathway Skyworth Router CM5100 v.4.1.1.24 allows a physically proximate attacker to obtain user credentials via SPI flash Firmware W25Q64JV.	4.6	More Details
CVE-2024-34653	Path Traversal in My Files prior to SMR Sep-2024 Release 1 allows physical attackers to access directories with My Files' privilege.	4.6	More Details
CVE-2024-34639	Improper handling of exceptional conditions in Setupwizard prior to SMR Aug-2024 Release 1 allows physical attackers to bypass proper validation.	4.6	More Details
CVE-2024-34642	Improper authorization in One UI Home prior to SMR Sep-2024 Release 1 allows physical attackers to temporarily access sensitive information.	4.6	More Details
CVE-2024-45447	Access control vulnerability in the camera framework module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	4.4	More Details
CVE-2022-3556	The Cab fare calculator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the vehicle title setting in versions up to, and including, 1.1.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with administrative privileges to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2024-7618	The Community by PeepSo – Social Network, Membership, Registration, User Profiles plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘content’ parameter in all versions up to, and including, 6.4.5.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2024-34643	Improper access control in key input related function in Dressroom prior to SMR Sep-2024 Release 1 allows local attackers to access protected data. User interaction is required for triggering this vulnerability.	4.4	More Details
CVE-2024-34644	Improper access control in item selection related in Dressroom prior to SMR Sep-2024 Release 1 allows local attackers to access protected data. User interaction is required for triggering this vulnerability.	4.4	More Details
CVE-2024-6876	Out-of-Bounds read vulnerability in OSCAT Basic Library allows an local, unprivileged attacker to access limited internal data of the PLC which may lead to a crash of the affected service.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7655	The Community by PeepSo – Social Network, Membership, Registration, User Profiles plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 6.4.5.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2024-27368	An issue was discovered in Samsung Mobile Processor Exynos Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_received_frame_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read.	4.4	More Details
CVE-2024-27366	An issue was discovered in Samsung Mobile Processor, Wearable Processor Exynos Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_done_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read.	4.4	More Details
CVE-2024-27364	An issue was discovered in Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_roamed_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read.	4.4	More Details
CVE-2023-30755	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions < V3.5.20), SIMATIC CP 1243-7 LTE (All versions < V3.5.20), SIMATIC CP 1243-8 IRC (6GK7243-8RX30-0XE0) (All versions < V3.5.20), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC IPC DiagBase (All versions), SIMATIC IPC DiagMonitor (All versions), SIMATIC WinCC Runtime Advanced (All versions), SIPLUS TIM 1531 IRC (6AG1543-1MX00-7XE0) (All versions < V2.4.8), TIM 1531 IRC (6GK7543-1MX00-0XE0) (All versions < V2.4.8). The web server of the affected devices do not properly handle the shutdown or reboot request, which could lead to the clean up of certain resources. This could allow a remote attacker with elevated privileges to cause a denial of service condition in the system.	4.4	More Details
CVE-2024-27367	An issue was discovered in Samsung Mobile Processor Exynos Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_ind(), there is no input validation check on a length coming from userspace, which can lead to integer overflow and a potential heap over-read.	4.4	More Details
CVE-2024-42344	A vulnerability has been identified in SINEMA Remote Connect Client (All versions < V3.2 SP2). The affected application inserts sensitive information into a log file which is readable by all legitimate users of the underlying system. This could allow an authenticated attacker to compromise the confidentiality of other users' configuration data.	4.4	More Details
CVE-2024-27365	An issue was discovered in Samsung Mobile Processor Exynos Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_blockack_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read.	4.4	More Details
CVE-2023-45038	An improper authentication vulnerability has been reported to affect Music Station. If exploited, the vulnerability could allow users to compromise the security of the system via a network. We have already fixed the vulnerability in the following version: Music Station 5.4.0 and later	4.3	More Details
CVE-2024-8427	The Frontend Post Submission Manager Lite – Frontend Posting WordPress Plugin plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the save_global_settings and process_form_edit functions in all versions up to, and including, 1.2.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update the plugin's settings and forms.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7622	The Revision Manager TMC plugin for WordPress is vulnerable to unauthorized arbitrary email sending due to a missing capability check on the _a_ajaxQuickEmailTestCallback() function in all versions up to, and including, 2.8.19. This makes it possible for authenticated attackers, with subscriber-level access and above, to send emails with arbitrary content to any individual through the vulnerable web server.	4.3	More Details
CVE-2024-32006	A vulnerability has been identified in SINEMA Remote Connect Client (All versions < V3.2 SP2). The affected application does not expire the user session on reboot without logout. This could allow an attacker to bypass Multi-Factor Authentication.	4.3	More Details
CVE-2024-6856	The WP MultiTasking WordPress plugin through 0.1.12 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	4.3	More Details
CVE-2023-50366	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later	4.3	More Details
CVE-2023-2919	The Tutor LMS plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.7.4. This is due to missing or incorrect nonce validation on the 'addon_enable_disable' function. This makes it possible for unauthenticated attackers to enable or disable addons via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2024-34155	Calling any of the Parse functions on Go source code which contains deeply nested literals can cause a panic due to stack exhaustion.	4.3	More Details
CVE-2024-8521	A vulnerability, which was classified as problematic, was found in Wavelog up to 1.8.0. Affected is the function index of the file /qso of the component Live QSO. The manipulation of the argument manual 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. Upgrading to version 1.8.1 is able to address this issue. The patch is identified as b31002cec6b71ab5f738881806bb546430ec692e. It is recommended to upgrade the affected component.	4.3	More Details
CVE-2024-8538	The Big File Uploads – Increase Maximum File Upload Size plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 2.1.2. This is due the plugin not sanitizing a file path in an error message. This makes it possible for authenticated attackers, with author-level access and above, to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	4.3	More Details
CVE-2024-44082	In OpenStack Ironic before 26.0.1 and ironic-python-agent before 9.13.1, there is a vulnerability in image processing, in which a crafted image could be used by an authenticated user to exploit undesired behaviors in qemu-img, including possible unauthorized access to potentially sensitive data. The affected/fixed version details are: Ironic: <21.4.3, >=22.0.0 <23.0.2, >=23.1.0 <24.1.2, >=25.0.0 <26.0.1; Ironic-python-agent: <9.4.2, >=9.5.0 <9.7.1, >=9.8.0 <9.11.1, >=9.12.0 <9.13.1.	4.3	More Details
CVE-2024-41729	Due to missing authorization checks, SAP BEx Analyzer allows an authenticated attacker to access information over the network which is otherwise restricted. On successful exploitation the attacker can enumerate information causing a limited impact on confidentiality of the application.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37994	A vulnerability has been identified in SIMATIC Reader RF610R CMIIT (6GT2811-6BC10-2AA0) (All versions < V4.2), SIMATIC Reader RF610R ETSI (6GT2811-6BC10-0AA0) (All versions < V4.2), SIMATIC Reader RF610R FCC (6GT2811-6BC10-1AA0) (All versions < V4.2), SIMATIC Reader RF615R CMIIT (6GT2811-6CC10-2AA0) (All versions < V4.2), SIMATIC Reader RF615R ETSI (6GT2811-6CC10-0AA0) (All versions < V4.2), SIMATIC Reader RF615R FCC (6GT2811-6CC10-1AA0) (All versions < V4.2), SIMATIC Reader RF650R ARIB (6GT2811-6AB20-4AA0) (All versions < V4.2), SIMATIC Reader RF650R CMIIT (6GT2811-6AB20-2AA0) (All versions < V4.2), SIMATIC Reader RF650R ETSI (6GT2811-6AB20-0AA0) (All versions < V4.2), SIMATIC Reader RF650R FCC (6GT2811-6AB20-1AA0) (All versions < V4.2), SIMATIC Reader RF680R ARIB (6GT2811-6AA10-4AA0) (All versions < V4.2), SIMATIC Reader RF680R CMIIT (6GT2811-6AA10-2AA0) (All versions < V4.2), SIMATIC Reader RF680R ETSI (6GT2811-6AA10-0AA0) (All versions < V4.2), SIMATIC Reader RF680R FCC (6GT2811-6AA10-1AA0) (All versions < V4.2), SIMATIC Reader RF685R ARIB (6GT2811-6CA10-4AA0) (All versions < V4.2), SIMATIC Reader RF685R CMIIT (6GT2811-6CA10-2AA0) (All versions < V4.2), SIMATIC Reader RF685R ETSI (6GT2811-6CA10-0AA0) (All versions < V4.2), SIMATIC Reader RF685R FCC (6GT2811-6CA10-1AA0) (All versions < V4.2), SIMATIC RF1140R (6GT2831-6CB00) (All versions < V1.1), SIMATIC RF1170R (6GT2831-6BB00) (All versions < V1.1), SIMATIC RF166C (6GT2002-0EE20) (All versions < V2.2), SIMATIC RF185C (6GT2002-0JE10) (All versions < V2.2), SIMATIC RF186C (6GT2002-0JE20) (All versions < V2.2), SIMATIC RF186CI (6GT2002-0JE50) (All versions < V2.2), SIMATIC RF188C (6GT2002-0JE40) (All versions < V2.2), SIMATIC RF188CI (6GT2002-0JE60) (All versions < V2.2), SIMATIC RF360R (6GT2801-5BA30) (All versions < V2.2). The affected application contains a hidden configuration item to enable debug functionality. This could allow an attacker to gain insight into the internal configuration of the deployment.	4.3	More Details
CVE-2024-42380	The RFC enabled function module allows a low privileged user to read any user's workplace favourites and user menu along with all the specific data of each node. Usernames can be enumerated by exploiting vulnerability. There is low impact on confidentiality of the application.	4.3	More Details
CVE-2024-8409	A vulnerability classified as problematic has been found in ABCD ABCD2 up to 2.2.0-beta-1. This affects an unknown part of the file /common/show_image.php. The manipulation of the argument image leads to path traversal: '../filedir'. 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-2024-8410	A vulnerability classified as problematic was found in ABCD ABCD2 up to 2.2.0-beta-1. This vulnerability affects unknown code of the file /abcd/opac/php/otros_sitios.php. The manipulation of the argument sitio leads to path traversal. 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.	4.3	More Details
CVE-2024-8412	A vulnerability, which was classified as problematic, was found in LinuxOSsk Shakal-NG up to 1.3.3. Affected is an unknown function of the file comments/views.py. The manipulation of the argument next leads to open redirect. It is possible to launch the attack remotely. The name of the patch is ebd1c2cba59cbac198bf2fd5a10565994d4f02cb. It is recommended to apply a patch to fix this issue.	4.3	More Details
CVE-2024-20497	A vulnerability in Cisco Expressway Edge (Expressway-E) could allow an authenticated, remote attacker to masquerade as another user on an affected system. This vulnerability is due to inadequate authorization checks for Mobile and Remote Access (MRA) users. An attacker could exploit this vulnerability by running a series of crafted commands. A successful exploit could allow the attacker to intercept calls that are destined for a particular phone number or to make phone calls and have that phone number appear on the caller ID. To successfully exploit this vulnerability, the attacker must be an MRA user on an affected system.	4.3	More Details
CVE-2024-8414	A vulnerability has been found in SourceCodester Insurance Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44121	Under certain conditions Statutory Reports in SAP S/4 HANA allows an attacker with basic privileges to access information which would otherwise be restricted. The vulnerability could expose internal user data that should remain confidential. It does not impact the integrity and availability of the application	4.3	More Details
CVE-2024-0067	Marinus Pfund, member of the AXIS OS Bug Bounty Program, has found the VAPIX API ledlimit.cgi was vulnerable for path traversal attacks allowing to list folder/file names on the local file system of the Axis device. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution.	4.3	More Details
CVE-2024-44112	Due to missing authorization check in SAP for Oil & Gas (Transportation and Distribution), an attacker authenticated as a non-administrative user could call a remote-enabled function which will allow them to delete non-sensitive entries in a user data table. There is no effect on confidentiality or availability.	4.3	More Details
CVE-2024-34661	Improper handling of insufficient permissions in Samsung Assistant prior to version 9.1.00.7 allows remote attackers to access location data. User interaction is required for triggering this vulnerability.	4.3	More Details
CVE-2024-45399	Indico is an event management system that uses Flask-Multipass, a multi-backend authentication system for Flask. In Indico prior to version 3.3.4, corresponding to Flask-Multipass prior to version 0.5.5, there is a Cross-Site-Scripting vulnerability during account creation when redirecting to the \`next\` URL. Exploitation requires initiating the account creation process with a maliciously crafted link, and then finalizing the signup process. Because of this, it can only target newly created (and thus unprivileged) Indico users. Indico 3.3.4 upgrades the dependency on Flask-Multipass to version 0.5.5, which fixes the issue. Those who build the Indico package themselves and cannot upgrade can update the \`flask-multipass\` dependency to \`>=0.5.5\` which fixes the vulnerability. Otherwise one could configure one's web server to disallow requests containing a query string with a \`next\` parameter that starts with \`javascript:\`.	4.3	More Details
CVE-2024-44116	The RFC enabled function module allows a low privileged user to add any workbook to any user's workplace favourites. This vulnerability could be utilized to identify usernames and access information about targeted user's workplaces. There is low impact on integrity of the application.	4.3	More Details
CVE-2024-44115	The RFC enabled function module allows a low privileged user to add URLs to any user's workplace favourites. This vulnerability could be utilized to identify usernames and access information about targeted user's workplaces, and nodes. There is low impact on integrity of the application	4.3	More Details
CVE-2024-7380	The Geo Controller plugin for WordPress is vulnerable to unauthorized menu creation/deletion due to missing capability checks on the ajax__geolocate_menu and ajax__geolocate_remove_menu functions in all versions up to, and including, 8.6.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create or delete WordPress menus.	4.3	More Details
CVE-2024-44113	Due to missing authorization checks, SAP Business Warehouse (BEx Analyzer) allows an authenticated attacker to access information over the network which is otherwise restricted. On successful exploitation the attacker can enumerate information causing a limited impact on confidentiality of the application.	4.3	More Details
CVE-2024-7605	The HelloAsso plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ha_ajax' function in all versions up to, and including, 1.1.10. This makes it possible for authenticated attackers, with Contributor-level access and above, to update plugin options, potentially disrupting the service.	4.3	More Details
CVE-2024-8555	A vulnerability was found in SourceCodester Clinics Patient Management System 2.0. It has been classified as problematic. Affected is an unknown function of the file congratulations.php. The manipulation of the argument goto_page leads to open redirect. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8322	Weak authentication in Patch Management of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker to access restricted functionality.	4.3	More Details
CVE-2024-31490	An exposure of sensitive information to an unauthorized actor in Fortinet FortiSandbox version 4.4.0 through 4.4.4 and 4.2.0 through 4.2.6 and 4.0.0 through 4.0.5 and 3.2.2 through 3.2.4 and 3.1.5 allows attacker to information disclosure via HTTP get requests.	4.3	More Details
CVE-2024-6852	The WP MultiTasking WordPress plugin through 0.1.12 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	4.3	More Details
CVE-2024-42342	Loway - CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')	4.3	More Details
CVE-2024-7687	The AZIndex WordPress plugin through 0.8.1 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack.	4.3	More Details
CVE-2024-6855	The WP MultiTasking WordPress plugin through 0.1.12 does not have CSRF check when updating exit popups, which could allow attackers to make logged admins perform such action via a CSRF attack	4.3	More Details
CVE-2024-7689	The Snapshot Backup WordPress plugin through 2.1.1 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack.	4.3	More Details
CVE-2024-42039	Access control vulnerability in the SystemUI module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	4.3	More Details
CVE-2024-45203	Improper authorization in handler for custom URL scheme issue in "@cosme" App for Android versions prior 5.69.0 and "@cosme" App for iOS versions prior to 6.74.0 allows an attacker to lead a user to access an arbitrary website via the vulnerable App. As a result, the user may become a victim of a phishing attack.	4.3	More Details
CVE-2024-8566	A vulnerability classified as problematic was found in code-projects Online Shop Store 1.0. This vulnerability affects unknown code of the file /settings.php. The manipulation of the argument error leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2024-8604	A vulnerability classified as problematic has been found in SourceCodester Online Food Ordering System 2.0. This affects an unknown part of the file index.php of the component Create an Account Page. The manipulation of the argument First Name/Last Name leads to cross site scripting. It is possible to initiate the attack remotely.	4.3	More Details
CVE-2024-45323	An improper access control vulnerability [CWE-284] in FortiEDR Manager API 6.2.0 through 6.2.2, 6.0 all versions may allow in a shared environment context an authenticated admin with REST API permissions in his profile and restricted to a specific organization to access backend logs that include information related to other organizations.	4.3	More Details
CVE-2024-8605	A vulnerability classified as problematic was found in code-projects Inventory Management 1.0. This vulnerability affects unknown code of the file /view/registration.php of the component Registration Form. The manipulation with the input <script>alert(1)</script> leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6853	The WP MultiTasking WordPress plugin through 0.1.12 does not have CSRF check when updating welcome popups, which could allow attackers to make logged admins perform such action via a CSRF attack	4.3	More Details
CVE-2024-42345	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP2). The affected application does not properly handle user session establishment and invalidation. This could allow a remote attacker to circumvent the additional multi factor authentication for user session establishment.	4.3	More Details
CVE-2024-27257	IBM OpenPages 8.3 and 9.0 potentially exposes information about client-side source code through use of JavaScript source maps to unauthorized users.	4.3	More Details
CVE-2024-8558	A vulnerability classified as problematic was found in SourceCodester Food Ordering Management System 1.0. This vulnerability affects unknown code of the file /foms/routers/place-order.php of the component Price Handler. The manipulation of the argument total leads to improper validation of specified quantity in input. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2024-6925	The TrueBooker WordPress plugin before 1.0.3 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack.	4.3	More Details
CVE-2024-35282	A cleartext storage of sensitive information in memory vulnerability [CWE-316] affecting FortiClient VPN iOS 7.2 all versions, 7.0 all versions, 6.4 all versions, 6.2 all versions, 6.0 all versions may allow an unauthenticated attacker that has physical access to a jailbroken device to obtain cleartext passwords via keychain dump.	4.2	More Details
CVE-2024-39278	Credentials to access device configuration information stored unencrypted in flash memory. These credentials would allow read-only access to network configuration information and terminal configuration data.	4.2	More Details
CVE-2024-45448	Page table protection configuration vulnerability in the trusted firmware module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	4.1	More Details
CVE-2024-45445	Vulnerability of resources not being closed or released in the keystore module Impact: Successful exploitation of this vulnerability will affect availability.	4.0	More Details
CVE-2024-34658	Out-of-bounds read in Samsung Notes allows local attackers to bypass ASLR.	4.0	More Details
CVE-2024-20505	A vulnerability in the PDF parsing module of Clam AntiVirus (ClamAV) versions 1.4.0, 1.3.2 and prior versions, all 1.2.x versions, 1.0.6 and prior versions, all 0.105.x versions, all 0.104.x versions, and 0.103.11 and all prior versions could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to an out of bounds read. An attacker could exploit this vulnerability by submitting a crafted PDF file to be scanned by ClamAV on an affected device. An exploit could allow the attacker to terminate the scanning process.	4.0	More Details
CVE-2024-45450	Permission control vulnerability in the software update module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	4.0	More Details
CVE-2024-34650	Incorrect authorization in CocktailbarService prior to SMR Sep-2024 Release 1 allows local attackers to access privileged APIs related to Edge panel.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34652	Incorrect authorization in kperfmon prior to SMR Sep-2024 Release 1 allows local attackers to access information related to performance including app usage.	4.0	More Details
CVE-2024-34647	Incorrect use of privileged API in DualDarManagerProxy prior to SMR Sep-2024 Release 1 allows local attackers to access privileged APIs related to knox without proper license.	4.0	More Details
CVE-2024-42425	Dell Precision Rack, 14G Intel BIOS versions prior to 2.22.2, contains an Access of Memory Location After End of Buffer vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	3.8	More Details
CVE-2024-8460	A vulnerability, which was classified as problematic, has been found in D-Link DNS-320 2.02b01. Affected by this issue is some unknown functionality of the file /cgi-bin/widget_api.cgi of the component Web Management Interface. The manipulation of the argument getHD/getSer/getSys leads to information disclosure. 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. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	3.7	More Details
CVE-2024-36511	An improperly implemented security check for standard vulnerability [CWE-358] in FortiADC Web Application Firewall (WAF) 7.4.0 through 7.4.4, 7.2 all versions, 7.1 all versions, 7.0 all versions, 6.2 all versions, 6.1 all versions, 6.0 all versions when cookie security policy is enabled may allow an attacker, under specific conditions, to retrieve the initial encrypted and signed cookie protected by the feature	3.7	More Details
CVE-2024-8462	A vulnerability was found in Windmill 1.380.0. It has been classified as problematic. Affected is an unknown function of the file backend/windmill-api/src/users.rs of the component HTTP Request Handler. The manipulation leads to improper restriction of excessive authentication attempts. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. Upgrading to version 1.390.1 is able to address this issue. The patch is identified as acfe7786152f036f2476f93ab5536571514fa9e3. It is recommended to upgrade the affected component.	3.7	More Details
CVE-2024-45314	Flask-AppBuilder is an application development framework. Prior to version 4.5.1, the auth DB login form default cache directives allows browser to locally store sensitive data. This can be an issue on environments using shared computer resources. Version 4.5.1 contains a patch for this issue. If upgrading is not possible, configure one's web server to send the specific HTTP headers for `/login` per the directions provided in the GitHub Security Advisory.	3.6	More Details
CVE-2024-6792	The WP ULike WordPress plugin before 4.7.2.1 does not properly sanitize user display names when rendering on a public page.	3.5	More Details
CVE-2024-27125	A cross-site scripting (XSS) vulnerability has been reported to affect Helpdesk. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following version: Helpdesk 3.3.1 and later	3.5	More Details
CVE-2024-8563	A vulnerability was found in SourceCodester PHP CRUD 1.0. It has been classified as problematic. This affects an unknown part of the file /endpoint/update.php. The manipulation of the argument first_name/middle_name/last_name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8411	A vulnerability, which was classified as problematic, has been found in ABCD ABCD2 up to 2.2.0-beta-1. This issue affects some unknown processing of the file /buscar_integrada.php. The manipulation of the argument Sub_Expresion 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-2024-8562	A vulnerability was found in SourceCodester PHP CRUD 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /endpoint/Add.php. The manipulation of the argument first_name/middle_name/last_name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-8571	A vulnerability was found in erjemin roll_cms up to 1484fe2c4e0805946a7bcf46218509fcb34883a9. It has been classified as problematic. This affects an unknown part of the file roll_cms/roll_cms/views.py. The manipulation leads to information exposure through error message. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available.	3.5	More Details
CVE-2024-8610	A vulnerability classified as problematic has been found in SourceCodester Best House Rental Management System 1.0. Affected is an unknown function of the file /index.php?page=tenants of the component New Tenant Page. The manipulation of the argument Last Name/First Name/Middle Name leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-8572	A vulnerability was found in Gouniverse GoLang CMS 1.4.0. It has been declared as problematic. This vulnerability affects the function PageRenderHtmlByAlias of the file FrontendHandler.go. The manipulation of the argument alias leads to cross site scripting. The attack can be initiated remotely. Upgrading to version 1.4.1 is able to address this issue. The patch is identified as 3e661cdfb4beeb9fe2ad507cdb8104c0b17d072c. It is recommended to upgrade the affected component.	3.5	More Details
CVE-2024-8583	A vulnerability was found in SourceCodester Online Bank Management System and Online Bank Management System - 1.0. It has been classified as problematic. This affects an unknown part of the file /mfeedback.php of the component Feedback Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-8554	A vulnerability was found in SourceCodester Clinics Patient Management System 2.0 and classified as problematic. This issue affects some unknown processing of the file /users.php. The manipulation of the argument message leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-8582	A vulnerability was found in SourceCodester Food Ordering Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /index.php. The manipulation of the argument description leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-8407	A vulnerability was found in alwindoss akademy up to 35caccea888ed63d5489e211c99edff1f62efdba. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file cmd/akademy/handler/handlers.go. The manipulation of the argument emailAddress leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.	3.5	More Details
CVE-2024-34640	Improper access control vulnerability in BGProtectManager prior to SMR Sep-2024 Release 1 allows local attackers to bypass restriction of process expiration.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45395	sigstore-go, a Go library for Sigstore signing and verification, is susceptible to a denial of service attack in versions prior to 0.6.1 when a verifier is provided a maliciously crafted Sigstore Bundle containing large amounts of verifiable data, in the form of signed transparency log entries, RFC 3161 timestamps, and attestation subjects. The verification of these data structures is computationally expensive. This can be used to consume excessive CPU resources, leading to a denial of service attack. TUF's security model labels this type of vulnerability an "Endless data attack," and can lead to verification failing to complete and disrupting services that rely on sigstore-go for verification. This vulnerability is addressed with sigstore-go 0.6.1, which adds hard limits to the number of verifiable data structures that can be processed in a bundle. Verification will fail if a bundle has data that exceeds these limits. The limits are 32 signed transparency log entries, 32 RFC 3161 timestamps, 1024 attestation subjects, and 32 digests per attestation subject. These limits are intended to be high enough to accommodate the vast majority of use cases, while preventing the verification of maliciously crafted bundles that contain large amounts of verifiable data. Users who are vulnerable but unable to quickly upgrade may consider adding manual bundle validation to enforce limits similar to those in the referenced patch prior to calling sigstore-go's verification functions.	3.1	More Details
CVE-2024-8417	A vulnerability was found in 云课网络科技有限公司 Yunke Online School System up to 1.5.5. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/educloud/videobind.html. The manipulation leads to inclusion of sensitive information in source code. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. Upgrading to version 1.5.6 is able to address this issue. It is recommended to upgrade the affected component.	3.1	More Details
CVE-2024-8443	A heap-based buffer overflow vulnerability was found in the libopensc OpenPGP driver. A crafted USB device or smart card with malicious responses to the APDUs during the card enrollment process using the `pkcs15-init` tool may lead to out-of-bound rights, possibly resulting in arbitrary code execution.	2.9	More Details
CVE-2024-37995	A vulnerability has been identified in SIMATIC Reader RF610R CMIIT (6GT2811-6BC10-2AA0) (All versions < V4.2), SIMATIC Reader RF610R ETSI (6GT2811-6BC10-0AA0) (All versions < V4.2), SIMATIC Reader RF610R FCC (6GT2811-6BC10-1AA0) (All versions < V4.2), SIMATIC Reader RF615R CMIIT (6GT2811-6CC10-2AA0) (All versions < V4.2), SIMATIC Reader RF615R ETSI (6GT2811-6CC10-0AA0) (All versions < V4.2), SIMATIC Reader RF615R FCC (6GT2811-6CC10-1AA0) (All versions < V4.2), SIMATIC Reader RF650R ARIB (6GT2811-6AB20-4AA0) (All versions < V4.2), SIMATIC Reader RF650R CMIIT (6GT2811-6AB20-2AA0) (All versions < V4.2), SIMATIC Reader RF650R ETSI (6GT2811-6AB20-0AA0) (All versions < V4.2), SIMATIC Reader RF650R FCC (6GT2811-6AB20-1AA0) (All versions < V4.2), SIMATIC Reader RF680R ARIB (6GT2811-6AA10-4AA0) (All versions < V4.2), SIMATIC Reader RF680R CMIIT (6GT2811-6AA10-2AA0) (All versions < V4.2), SIMATIC Reader RF680R ETSI (6GT2811-6AA10-0AA0) (All versions < V4.2), SIMATIC Reader RF680R FCC (6GT2811-6AA10-1AA0) (All versions < V4.2), SIMATIC Reader RF685R ARIB (6GT2811-6CA10-4AA0) (All versions < V4.2), SIMATIC Reader RF685R CMIIT (6GT2811-6CA10-2AA0) (All versions < V4.2), SIMATIC Reader RF685R ETSI (6GT2811-6CA10-0AA0) (All versions < V4.2), SIMATIC Reader RF685R FCC (6GT2811-6CA10-1AA0) (All versions < V4.2), SIMATIC RF1140R (6GT2831-6CB00) (All versions < V1.1), SIMATIC RF1170R (6GT2831-6BB00) (All versions < V1.1), SIMATIC RF166C (6GT2002-0EE20) (All versions < V2.2), SIMATIC RF185C (6GT2002-0JE10) (All versions < V2.2), SIMATIC RF186C (6GT2002-0JE20) (All versions < V2.2), SIMATIC RF186CI (6GT2002-0JE50) (All versions < V2.2), SIMATIC RF188C (6GT2002-0JE40) (All versions < V2.2), SIMATIC RF188CI (6GT2002-0JE60) (All versions < V2.2), SIMATIC RF360R (6GT2801-5BA30) (All versions < V2.2). The affected application improperly handles error while a faulty certificate upload leading to crashing of application. This vulnerability could allow an attacker to disclose sensitive information.	2.7	More Details
CVE-2024-41728	Due to missing authorization check, SAP NetWeaver Application Server for ABAP and ABAP Platform allows an attacker logged in as a developer to read objects contained in a package. This causes an impact on confidentiality, as this attacker would otherwise not have access to view these objects.	2.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-32771	An improper restriction of excessive authentication attempts vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow local network authenticated administrators to perform an arbitrary number of authentication attempts via unspecified vectors. QuTScloud is not affected. We have already fixed the vulnerability in the following versions: QTS 5.2.0.2782 build 20240601 and later QuTS hero h5.2.0.2782 build 20240601 and later	2.6	More Details
CVE-2024-45284	An authenticated attacker with high privilege can use functions of SLCM transactions to which access should be restricted. This may result in an escalation of privileges causing low impact on integrity of the application.	2.4	More Details
CVE-2024-8042	Rapid7 Insight Platform versions between November 2019 and August 14, 2024 suffer from missing authorization issues whereby an attacker can intercept local requests to set the name and description of a new user group. This could potentially lead to an empty user group being added to the incorrect customer. This vulnerability is remediated as of August 14, 2024.	2.4	More Details
CVE-2024-34649	Improper access control in new Dex Mode in multitasking framework prior to SMR Sep-2024 Release 1 allows physical attackers to temporarily access an unlocked screen.	2.4	More Details
CVE-2024-39582	Dell PowerScale InsightIQ, version 5.0, contain a Use of hard coded Credentials vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	2.3	More Details
CVE-2024-44114	SAP NetWeaver Application Server for ABAP and ABAP Platform allow users with high privileges to execute a program that reveals data over the network. This results in a minimal impact on confidentiality of the application.	2.0	More Details
CVE-2024-39715	A code injection vulnerability that allows a low-privileged user with REST API access granted to remotely upload arbitrary files to the VSPC server using REST API, leading to remote code execution on VSPC server.	N/A	More Details
CVE-2024-7821	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-44948	In the Linux kernel, the following vulnerability has been resolved: x86/mtrr: Check if fixed MTRRs exist before saving them MTRRs have an obsolete fixed variant for fine grained caching control of the 640K-1MB region that uses separate MSRs. This fixed variant has a separate capability bit in the MTRR capability MSR. So far all x86 CPUs which support MTRR have this separate bit set, so it went unnoticed that mtrr_save_state() does not check the capability bit before accessing the fixed MTRR MSRs. Though on a CPU that does not support the fixed MTRR capability this results in a #GP. The #GP itself is harmless because the RDMSR fault is handled gracefully, but results in a WARN_ON(). Add the missing capability check to prevent this.	N/A	More Details
CVE-2024-45845	Rejected reason: DO NOT USE THIS CVE RECORD. Consult IDs: CVE-2024-45593. Reason: This record is a reservation duplicate of CVE-2024-45593. Notes: All CVE users should reference CVE-2024-45593 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-42024	A vulnerability that allows an attacker in possession of the Veeam ONE Agent service account credentials to perform remote code execution on the machine where the Veeam ONE Agent is installed.	N/A	More Details
CVE-2024-42023	An improper access control vulnerability allows low-privileged users to execute code with Administrator privileges remotely.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42022	An incorrect permission assignment vulnerability allows an attacker to modify product configuration files.	N/A	More Details
CVE-2024-42021	An improper access control vulnerability allows an attacker with valid access tokens to access saved credentials.	N/A	More Details
CVE-2024-42019	A vulnerability that allows an attacker to access the NTLM hash of the Veeam Reporter Service service account. This attack requires user interaction and data collected from Veeam Backup & Replication.	N/A	More Details
CVE-2024-40718	A server side request forgery vulnerability allows a low-privileged user to perform local privilege escalation through exploiting an SSRF vulnerability.	N/A	More Details
CVE-2024-40714	An improper certificate validation vulnerability in TLS certificate validation allows an attacker on the same network to intercept sensitive credentials during restore operations.	N/A	More Details
CVE-2024-40713	A vulnerability that allows a user who has been assigned a low-privileged role within Veeam Backup & Replication to alter Multi-Factor Authentication (MFA) settings and bypass MFA.	N/A	More Details
CVE-2024-40712	A path traversal vulnerability allows an attacker with a low-privileged account and local access to the system to perform local privilege escalation (LPE).	N/A	More Details
CVE-2024-40710	A series of related high-severity vulnerabilities, the most notable enabling remote code execution (RCE) as the service account and extraction of sensitive information (savedcredentials and passwords). Exploiting these vulnerabilities requires a user who has been assigned a low-privileged role within Veeam Backup & Replication.	N/A	More Details
CVE-2024-40709	A missing authorization vulnerability allows a local low-privileged user on the machine to escalate their privileges to root level.	N/A	More Details
CVE-2024-39714	A code injection vulnerability that permits a low-privileged user to upload arbitrary files to the server, leading to remote code execution on VSPC server.	N/A	More Details
CVE-2024-38651	A code injection vulnerability can allow a low-privileged user to overwrite files on that VSPC server, which can lead to remote code execution on VSPC server.	N/A	More Details
CVE-2024-38650	An authentication bypass vulnerability can allow a low privileged attacker to access the NTLM hash of service account on the VSPC server.	N/A	More Details
CVE-2024-36138	Bypass incomplete fix of CVE-2024-27980, that arises from improper handling of batch files with all possible extensions on Windows via child_process.spawn / child_process.spawnSync. A malicious command line argument can inject arbitrary commands and achieve code execution even if the shell option is not enabled.	N/A	More Details
CVE-2024-36137	A vulnerability has been identified in Node.js, affecting users of the experimental permission model when the --allow-fs-write flag is used. Node.js Permission Model do not operate on file descriptors, however, operations such as fs.fchown or fs.fchmod can use a "read-only" file descriptor to change the owner and permissions of a file.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8439	Rejected reason: Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that the issue does not pose a security risk as it falls within the expected functionality and security controls of the application.	N/A	More Details
CVE-2024-45295	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-45294. Reason: This candidate is a duplicate of CVE-2024-45294. Notes: All CVE users should reference CVE-2024-45294 instead of this candidate. This CVE was issued to a vulnerability that is dependent on CVE-2024-45294. According to rule 4.2.15 of the CVE CNA rules, "CNAs MUST NOT assign a different CVE ID to a Vulnerability that is fully interdependent with another Vulnerability. The Vulnerabilities are effectively the same single Vulnerability and MUST use one CVE ID."	N/A	More Details
CVE-2023-52916	In the Linux kernel, the following vulnerability has been resolved: media: aspeed: Fix memory overwrite if timing is 1600x900 When capturing 1600x900, system could crash when system memory usage is tight. The way to reproduce this issue: 1. Use 1600x900 to display on host 2. Mount ISO through 'Virtual media' on OpenBMC's web 3. Run script as below on host to do sha continuously #!/bin/bash while [[1]]; do find /media -type f -printf '"%h/%f"\n' | xargs sha256sum done 4. Open KVM on OpenBMC's web The size of macro block captured is 8x8. Therefore, we should make sure the height of src-buf is 8 aligned to fix this issue.	N/A	More Details
CVE-2024-45008	In the Linux kernel, the following vulnerability has been resolved: Input: MT - limit max slots syzbot is reporting too large allocation at input_mt_init_slots(), for num_slots is supplied from userspace using ioctl(UI_DEV_CREATE). Since nobody knows possible max slots, this patch chose 1024.	N/A	More Details
CVE-2024-45007	In the Linux kernel, the following vulnerability has been resolved: char: xillybus: Don't destroy workqueue from work item running on it Triggered by a kref decrement, destroy_workqueue() may be called from within a work item for destroying its own workqueue. This illegal situation is averted by adding a module-global workqueue for exclusive use of the offending work item. Other work items continue to be queued on per-device workqueues to ensure performance.	N/A	More Details
CVE-2024-44952	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-39718	An improper input validation vulnerability that allows a low-privileged user to remotely remove files on the system with permissions equivalent to those of the service account.	N/A	More Details