SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 13 March 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-2024-22039	A vulnerability has been identified in Cerberus PRO EN Engineering Tool (All versions < IP8), Cerberus PRO EN Fire Panel FC72x IP6 (All versions < IP6 SR3), Cerberus PRO EN Fire Panel FC72x IP7 (All versions < IP7 SR5), Cerberus PRO EN X200 Cloud Distribution IP7 (All versions < V3.0.6602), Cerberus PRO EN X200 Cloud Distribution IP8 (All versions < V4.0.5016), Cerberus PRO EN X300 Cloud Distribution IP7 (All versions < V3.2.6601), Cerberus PRO EN X300 Cloud Distribution IP8 (All versions < V4.2.5015), Cerberus PRO UL Compact Panel FC922/924 (All versions < MP4), Cerberus PRO UL Engineering Tool (All versions < MP4), Cerberus PRO UL X300 Cloud Distribution (All versions < V4.3.0001), Desigo Fire Safety UL Compact Panel FC2025/2050 (All versions < MP4), Desigo Fire Safety UL Engineering Tool (All versions < MP4), Desigo Fire Safety UL X300 Cloud Distribution (All versions < V4.3.0001), Sinteso FS20 EN Engineering Tool (All versions < MP8), Sinteso FS20 EN Fire Panel FC20 MP6 (All versions < MP6 SR3), Sinteso FS20 EN Fire Panel FC20 MP7 (All versions < MP7 SR5), Sinteso FS20 EN X200 Cloud Distribution MP7 (All versions < V3.0.6602), Sinteso FS20 EN X200 Cloud Distribution MP8 (All versions < V4.0.5016), Sinteso FS20 EN X300 Cloud Distribution MP7 (All versions < V3.2.6601), Sinteso FS20 EN X300 Cloud Distribution MP8 (All versions < V4.2.5015), Sinteso Mobile (All versions < V3.0.0). The network communication library in affected systems does not validate the length of certain X.509 certificate attributes which might result in a stack-based buffer overflow. This could allow an unauthenticated remote attacker to execute code on the underlying operating system with root privileges.	10.0	More Details
CVE-2024-2044	pgAdmin <= 8.3 is affected by a path-traversal vulnerability while deserializing users' sessions in the session handling code. If the server is running on Windows, an unauthenticated attacker can load and deserialize remote pickle objects and gain code execution. If the server is running on POSIX/Linux, an authenticated attacker can upload pickle objects, deserialize them, and gain code execution.	9.9	More Details
CVE-2023-41313	The authentication method in Apache Doris versions before 2.0.0 was vulnerable to timing attacks. Users are recommended to upgrade to version 2.0.0 + or 1.2.8, which fixes this issue.	9.8	More Details
CVE-2023-49340	An issue was discovered in Newland Nquire 1000 Interactive Kiosk version NQ1000-II_G_V1.00.011, allows remote attackers to escalate privileges and bypass authentication via incorrect access control in the web management portal.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2184	Buffer overflow in identifier field of WSD probe request process of Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code.*:Satera MF740C Series/Satera MF640C Series/Satera LBP660C Series/Satera LBP620C Series firmware v12.07 and earlier, and Satera MF750C Series/Satera LBP670C Series firmware v03.09 and earlier sold in Japan.Color imageCLASS MF740C Series/Color imageCLASS MF640C Series/Color imageCLASS X MF1127C/Color imageCLASS LBP664Cdw/Color imageCLASS LBP622Cdw/Color imageCLASS X LBP1127C firmware v12.07 and earlier, and Color imageCLASS MF750C Series/Color imageCLASS X MF1333C/Color imageCLASS LBP674Cdw/Color imageCLASS X LBP1333C firmware v03.09 and earlier sold in US.i-SENSYS MF740C Series/i-SENSYS MF640C Series/C1127i Series/i-SENSYS LBP660C Series/i-SENSYS LBP620C Series/C1127P firmware v12.07 and earlier, and i-SENSYS MF750C Series/C1333i Series/i-SENSYS LBP673Cdw/C1333P firmware v03.09 and earlier sold in Europe.	9.8	More Details
CVE-2024-0039	In attp_build_value_cmd of att_protocol.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2024-27228	there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2024-25995	An unauthenticated remote attacker can modify configurations to perform a remote code execution due to a missing authentication for a critical function.	9.8	More Details
CVE-2022-32257	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2). The affected application consists of a web service that lacks proper access control for some of the endpoints. This could lead to unauthorized access to resources and potentially lead to code execution.	9.8	More Details
CVE-2023-38944	An issue in Multilaser RE160V firmware v12.03.01.09_pt and Multilaser RE163V firmware v12.03.01.10_pt allows attackers to bypass the access control and gain complete access to the application via modifying a HTTP header.	9.8	More Details
CVE-2024-25849	In the module "Make an offer" (makeanoffer) <= 1.7.1 from PrestaToolKit for PrestaShop, a guest can perform SQL injection via MakeOffers::checkUserExistingOffer()` and `MakeOffers::addUserOffer()` .	9.8	More Details
CVE-2024-28535	Tenda AC18 V15.03.05.05 has a stack overflow vulnerability in the mitInterface parameter of fromAddressNat function.	9.8	More Details
CVE-2024-28553	Tenda AC18 V15.03.05.05 has a stack overflow vulnerability in the entrys parameter fromAddressNat function.	9.8	More Details
CVE-2023-42789	A out-of-bounds write in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests.	9.8	More Details
CVE-2023-48788	A improper neutralization of special elements used in an sql command ('sql injection') in Fortinet FortiClientEMS version 7.2.0 through 7.2.2, FortiClientEMS 7.0.1 through 7.0.10 allows attacker to execute unauthorized code or commands via specially crafted packets.	9.8	More Details
CVE-2024-1301	SQL injection vulnerability in Badger Meter Monitool affecting versions 4.6.3 and earlier. A remote attacker could send a specially crafted SQL query to the server via the j_username parameter and retrieve the information stored in the database.	9.8	More Details
CVE-2024-1527	Unrestricted file upload vulnerability in CMS Made Simple, affecting version 2.2.14. This vulnerability allows an authenticated user to bypass the security measures of the upload functionality and potentially create a remote execution of commands via webshell.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21334	Open Management Infrastructure (OMI) Remote Code Execution Vulnerability	9.8	More Details
CVE-2024-21899	An improper authentication vulnerability has been reported to affect several QNAP operating system versions. 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 versions: QTS 5.1.3.2578 build 20231110 and later QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later	9.8	More Details
CVE-2023-46427	An issue was discovered in gpac version 2.3-DEV-rev588-g7edc40fee-master, allows remote attackers to execute arbitrary code, cause a denial of service (DoS), and obtain sensitive information via null pointer deference in gf_dash_setup_period component in media_tools/dash_client.c.	9.8	More Details
CVE-2024-25845	In the module "CD Custom Fields 4 Orders" (cdcustomfields4orders) <= 1.0.0 from Cleanpresta.com for PrestaShop, a guest can perform SQL injection in affected versions.	9.8	More Details
CVE-2024-28212	nGrinder before 3.5.9 uses old version of SnakeYAML, which could allow remote attacker to execute arbitrary code via unsafe deserialization.	9.8	More Details
CVE-2024-27304	pgx is a PostgreSQL driver and toolkit for Go. SQL injection can occur if an attacker can cause a single query or bind message to exceed 4 GB in size. An integer overflow in the calculated message size can cause the one large message to be sent as multiple messages under the attacker's control. The problem is resolved in v4.18.2 and v5.5.4. As a workaround, reject user input large enough to cause a single query or bind message to exceed 4 GB in size.	9.8	More Details
CVE-2024-27307	JSONata is a JSON query and transformation language. Starting in version 1.4.0 and prior to version 1.8.7 and 2.0.4, a malicious expression can use the transform operator to override properties on the `Object` constructor and prototype. This may lead to denial of service, remote code execution or other unexpected behavior in applications that evaluate user-provided JSONata expressions. This issue has been fixed in JSONata versions 1.8.7 and 2.0.4. Applications that evaluate user-provided expressions should update ASAP to prevent exploitation. As a workaround, one may apply the patch manually.	9.8	More Details
CVE-2023-49989	Hotel Booking Management v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at update.php.	9.8	More Details
CVE-2024-28211	nGrinder before 3.5.9 allows connection to malicious JMX/RMI server by default, which could be the cause of executing arbitrary code via RMI registry by remote attacker.	9.8	More Details
CVE-2024-22857	Heap based buffer flow in zlog v1.1.0 to v1.2.17 in zlog_rule_new().The size of record_name is MAXLEN_PATH(1024) + 1 but file_path may have data upto MAXLEN_CFG_LINE(MAXLEN_PATH*4) + 1. So a check was missing in zlog_rule_new() while copying the record_name from file_path + 1 which caused the buffer overflow. An attacker can exploit this vulnerability to overwrite the zlog_record_fn record_func function pointer to get arbitrary code execution or potentially cause remote code execution (RCE).	9.8	More Details
CVE-2023-41503	Student Enrollment In PHP v1.0 was discovered to contain a SQL injection vulnerability via the Login function.	9.8	More Details
CVE-2024-28213	nGrinder before 3.5.9 allows to accept serialized Java objects from unauthenticated users, which could allow remote attacker to execute arbitrary code via unsafe Java objects deserialization.	9.8	More Details
CVE-2024-28222	In Veritas NetBackup before 8.1.2 and NetBackup Appliance before 3.1.2, the BPCD process inadequately validates the file path, allowing an unauthenticated attacker to upload and execute a custom file.	9.8	More Details
CVE-2024-24093	SQL Injection vulnerability in Code-projects Scholars Tracking System 1.0 allows attackers to run arbitrary code via Personal Information Update information.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-47534	A improper neutralization of formula elements in a csv file in Fortinet FortiClientEMS version 7.2.0 through 7.2.2, 7.0.0 through 7.0.10, 6.4.0 through 6.4.9, 6.2.0 through 6.2.9, 6.0.0 through 6.0.8 allows attacker to execute unauthorized code or commands via specially crafted packets.	9.6	More Details
CVE-2023-50716	eProsima Fast DDS (formerly Fast RTPS) is a C++ implementation of the Data Distribution Service standard of the Object Management Group. Prior to versions 2.13.0, 2.12.2, 2.11.3, 2.10.3, and 2.6.7, an invalid DATA_FRAG Submessage causes a bad-free error, and the Fast-DDS process can be remotely terminated. If an invalid Data_Frag packet is sent, the `Inline_qos, SerializedPayload` member of object `ch` will attempt to release memory without initialization, resulting in a 'bad-free' error. Versions 2.13.0, 2.12.2, 2.11.3, 2.10.2, and 2.6.7 fix this issue.	9.6	More Details
CVE-2023-42662	JFrog Artifactory versions 7.59 and above, but below 7.59.18, 7.63.18, 7.68.19, 7.71.8 are vulnerable to an issue whereby user interaction with specially crafted URLs could lead to exposure of user access tokens due to improper handling of the CLI / IDE browser based SSO integration.	9.3	More Details
CVE-2024-25331	DIR-822 Rev. B Firmware v2.02KRB09 and DIR-822-CA Rev. B Firmware v2.03WWb01 suffer from a LAN-Side Unauthenticated Remote Code Execution (RCE) vulnerability elevated from HNAP Stack-Based Buffer Overflow.	9.3	More Details
CVE-2024-27207	Exported broadcast receivers allowing malicious apps to bypass broadcast protection.	9.1	More Details
CVE-2023-51786	An issue was discovered in Lustre versions 2.13.x, 2.14.x, and 2.15.x before 2.15.4, allows attackers to escalate privileges and obtain sensitive information via Incorrect Access Control.	9.1	More Details
CVE-2024-22127	SAP NetWeaver Administrator AS Java (Administrator Log Viewer plug-in) - version 7.50, allows an attacker with high privileges to upload potentially dangerous files which leads to command injection vulnerability. This would enable the attacker to run commands which can cause high impact on confidentiality, integrity and availability of the application.	9.1	More Details
CVE-2024-26580	Deserialization of Untrusted Data vulnerability in Apache InLong.This issue affects Apache InLong: from 1.8.0 through 1.10.0, the attackers can use the specific payload to read from an arbitrary file. Users are advised to upgrade to Apache InLong's 1.11.0 or cherry-pick [1] to solve it. [1] https://github.com/apache/inlong/pull/9673	9.1	More Details
CVE-2024-27302	go-zero is a web and rpc framework. Go-zero allows user to specify a CORS Filter with a configurable allows param - which is an array of domains allowed in CORS policy. However, the `isOriginAllowed` uses `strings.HasSuffix` to check the origin, which leads to bypass via a malicious domain. This vulnerability is capable of breaking CORS policy and thus allowing any page to make requests and/or retrieve data on behalf of other users. Version 1.4.4 fixes this issue.	9.1	More Details
CVE-2024-24767	CasaOS-UserService provides user management functionalities to CasaOS. Starting in version 0.4.4.3 and prior to version 0.4.7, CasaOS doesn't defend against password brute force attacks, which leads to having full access to the server. The web application lacks control over the login attempts. This vulnerability allows attackers to get super user-level access over the server. Version 0.4.7 contains a patch for this issue.	9.1	More Details
CVE-2023-49785	NextChat, also known as ChatGPT-Next-Web, is a cross-platform chat user interface for use with ChatGPT. Versions 2.11.2 and prior are vulnerable to server-side request forgery and cross-site scripting. This vulnerability enables read access to internal HTTP endpoints but also write access using HTTP POST, PUT, and other methods. Attackers can also use this vulnerability to mask their source IP by forwarding malicious traffic intended for other Internet targets through these open proxies. As of time of publication, no patch is available, but other mitigation strategies are available. Users may avoid exposing the application to the public internet or, if exposing the application to the internet, ensure it is an isolated network with no access to any other internal resources.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2005	In Blue Planet® products through 22.12, a misconfiguration in the SAML implementation allows for privilege escalation. Only products using SAML authentication are affected. Blue Planet® has released software updates that address this vulnerability for the affected products. Customers are advised to upgrade their Blue Planet products to the latest software version as soon as possible. The software updates can be downloaded from the Ciena Support Portal.	9.0	More Details
CVE-2024-21400	Microsoft Azure Kubernetes Service Confidential Container Elevation of Privilege Vulnerability	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-38945	Multilaser RE160 v5.07.51_pt_MTL01 and v5.07.52_pt_MTL01, Multilaser RE160V v12.03.01.08_pt and V12.03.01.09_pt, and Multilaser RE163V v12.03.01.08_pt allows attackers to bypass the access control and gain complete access to the application via supplying a crafted URL.	8.8	More Details
CVE-2024-0203	The Digits plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 8.4.1. This is due to missing nonce validation in the 'digits_save_settings' function. This makes it possible for unauthenticated attackers to modify the default role of registered users to elevate user privileges via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2024-2353	A vulnerability, which was classified as critical, has been found in Totolink X6000R 9.4.0cu.852_20230719. This issue affects the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi of the component shttpd. The manipulation of the argument ip leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256313 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-26159	Microsoft ODBC Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-1351	Under certain configurations of --tlsCAFile and tls.CAFile, MongoDB Server may skip peer certificate validation which may result in untrusted connections to succeed. This may effectively reduce the security guarantees provided by TLS and open connections that should have been closed due to failing certificate validation. This issue affects MongoDB Server v7.0 versions prior to and including 7.0.5, MongoDB Server v6.0 versions prior to and including 6.0.13, MongoDB Server v5.0 versions prior to and including 5.0.24 and MongoDB Server v4.4 versions prior to and including 4.4.28. Required Configuration : A server process will allow incoming connections to skip peer certificate validation if the server process was started with TLS enabled (net.tls.mode set to allowTLS, preferTLS, or requireTLS) and without a net.tls.CAFile configured.	8.8	More Details
CVE-2024-0670	Privilege escalation in windows agent plugin in Checkmk before 2.2.0p23, 2.1.0p40 and 2.0.0 (EOL) allows local user to escalate privileges	8.8	More Details
CVE-2024-28094	Chat functionality in Schoolbox application before version 23.1.3 is vulnerable to blind SQL Injection enabling the authenticated attackers to read, modify, and delete database records.	8.8	More Details
CVE-2024-26161	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1773	The PDF Invoices and Packing Slips For WooCommerce plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.3.7 via deserialization of untrusted input via the order_id parameter. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	8.8	More Details
CVE-2024-26198	Microsoft Exchange Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-26162	Microsoft ODBC Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-23717	In access_secure_service_from_temp_bond of btm_sec.cc, there is a possible way to achieve keystroke injection due to improper input validation. This could lead to remote (proximal/adjacent) escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.8	More Details
CVE-2024-26164	Microsoft Django Backend for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-26165	Visual Studio Code Elevation of Privilege Vulnerability	8.8	More Details
CVE-2024-1986	The Booster Elite for WooCommerce plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the wc_add_new_product() function in all versions up to, and including, 7.1.7. This makes it possible for customer-level attackers, and above, to upload arbitrary files on the affected site's server which may make remote code execution possible. This is only exploitable when the user product upload functionality is enabled.	8.8	More Details
CVE-2024-2216	A missing permission check in an HTTP endpoint in Jenkins docker-build-step Plugin 2.11 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified TCP or Unix socket URL, and to reconfigure the plugin using the provided connection test parameters, affecting future build step executions.	8.8	More Details
CVE-2024-2174	Inappropriate implementation in V8 in Google Chrome prior to 122.0.6261.111 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-21411	Skype for Consumer Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-28115	FreeRTOS is a real-time operating system for microcontrollers. FreeRTOS Kernel versions through 10.6.1 do not sufficiently protect against local privilege escalation via Return Oriented Programming techniques should a vulnerability exist that allows code injection and execution. These issues affect ARMv7-M MPU ports, and ARMv8-M ports with Memory Protected Unit (MPU) support enabled (i.e. `configENABLE_MPU` set to 1). These issues are fixed in version 10.6.2 with a new MPU wrapper.	8.8	More Details
CVE-2024-26166	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-21451	Microsoft ODBC Driver Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25501	An issue WinMail v.7.1 and v.5.1 and before allows a remote attacker to execute arbitrary code via a crafted script to the email parameter.	8.8	More Details
CVE-2024-1138	The FTL Server component of TIBCO Software Inc.'s TIBCO FTL - Enterprise Edition contains a vulnerability that allows a low privileged attacker with network access to execute a privilege escalation on the affected ftlserver. Affected releases are TIBCO Software Inc.'s TIBCO FTL - Enterprise Edition: versions 6.10.1 and below.	8.8	More Details
CVE-2024-2173	Out of bounds memory access in V8 in Google Chrome prior to 122.0.6261.111 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-43318	TP-Link JetStream Smart Switch TL-SG2210P 5.0 Build 20211201 allows attackers to escalate privileges via modification of the 'tid' and 'usrlvl' values in GET requests.	8.8	More Details
CVE-2024-23226	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.4, visionOS 1.1, iOS 17.4 and iPadOS 17.4, watchOS 10.4, tvOS 17.4. Processing web content may lead to arbitrary code execution.	8.8	More Details
CVE-2024-21435	Windows OLE Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-46499	Hospital Management System 1.0 was discovered to contain a SQL injection vulnerability via the pat_number parameter at his_admin_view_single_patient.php.	8.8	More Details
CVE-2024-28160	Jenkins iceScrum Plugin 1.1.6 and earlier does not sanitize iceScrum project URLs on build views, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to configure jobs.	8.8	More Details
CVE-2024-1382	The Restaurant Reservations plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.9 via the nd_rst_layout attribute of the nd_rst_search shortcode. This makes it possible for authenticated attackers, with contributor-level access and above, to include and execute arbitrary PHP files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where an uploaded PHP file may not be directly accessible.	8.8	More Details
CVE-2023-50015	An issue was discovered in Grandstream GXP14XX 1.0.8.9 and GXP16XX 1.0.7.13, allows remote attackers to escalate privileges via incorrect access control using an end-user session-identity token.	8.8	More Details
CVE-2023-46426	Heap-based Buffer Overflow vulnerability in gpac version 2.3-DEV-rev588-g7edc40fee-master, allows remote attackers to execute arbitrary code and cause a denial of service (DoS) via gf_fwrite component in at utils/os_file.c.	8.8	More Details
CVE-2024-21440	Microsoft ODBC Driver Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28121	stimulus_reflex is a system to extend the capabilities of both Rails and Stimulus by intercepting user interactions and passing them to Rails over real-time websockets. In affected versions more methods than expected can be called on reflex instances. Being able to call some of them has security implications. To invoke a reflex a websocket message of the following shape is sent: `\"target\":\"[class_name]#[method_name]\",\"args\":[]`. The server will proceed to instantiate `reflex` using the provided `class_name` as long as it extends `StimulusReflex::Reflex`. It then attempts to call `method_name` on the instance with the provided arguments. This is problematic as `reflex.method method_name` can be more methods that those explicitly specified by the developer in their reflex class. A good example is the instance_variable_set method. This vulnerability has been patched in versions 3.4.2 and 3.5.0.rc4. Users unable to upgrade should: see the backing GHSA advisory for mitigation advice.	8.8	More Details
CVE-2023-51395	The vulnerability described by CVE-2023-0972 has been additionally discovered in Silicon Labs Z-Wave end devices. This vulnerability may allow an unauthenticated attacker within Z-Wave range to overflow a stack buffer, leading to arbitrary code execution.	8.8	More Details
CVE-2024-21441	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-38946	An issue in Multilaser RE160 firmware v5.07.51_pt_MTL01 and v5.07.52_pt_MTL01 allows attackers to bypass the access control and gain complete access to the application via supplying a crafted cookie.	8.8	More Details
CVE-2024-21444	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-25729	Arris SBG6580 devices have predictable default WPA2 security passwords that could lead to unauthorized remote access. (They use the first 6 characters of the SSID and the last 6 characters of the BSSID, decrementing the last octet.)	8.8	More Details
CVE-2024-21450	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-2176	Use after free in FedCM in Google Chrome prior to 122.0.6261.111 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-26288	An unauthenticated remote attacker can influence the communication due to the lack of encryption of sensitive data via a MITM. Charging is not affected.	8.7	More Details
CVE-2024-25111	Squid is a web proxy cache. Starting in version 3.5.27 and prior to version 6.8, Squid may be vulnerable to a Denial of Service attack against HTTP Chunked decoder due to an uncontrolled recursion bug. This problem allows a remote attacker to cause Denial of Service when sending a crafted, chunked, encoded HTTP Message. This bug is fixed in Squid version 6.8. In addition, patches addressing this problem for the stable releases can be found in Squid's patch archives. There is no workaround for this issue.	8.6	More Details
CVE-2024-23246	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14.4, visionOS 1.1, iOS 17.4 and iPadOS 17.4, watchOS 10.4, iOS 16.7.6 and iPadOS 16.7.6, tvOS 17.4. An app may be able to break out of its sandbox.	8.6	More Details
CVE-2024-0258	The issue was addressed with improved memory handling. This issue is fixed in tvOS 17.4, iOS 17.4 and iPadOS 17.4, macOS Sonoma 14.4, watchOS 10.4. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23278	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.6.5, macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4, watchOS 10.4, iOS 16.7.6 and iPadOS 16.7.6, tvOS 17.4. An app may be able to break out of its sandbox.	8.6	More Details
CVE-2024-27894	The Pulsar Functions Worker includes a capability that permits authenticated users to create functions where the function's implementation is referenced by a URL. The supported URL schemes include "file", "http", and "https". When a function is created using this method, the Functions Worker will retrieve the implementation from the URL provided by the user. However, this feature introduces a vulnerability that can be exploited by an attacker to gain unauthorized access to any file that the Pulsar Functions Worker process has permissions to read. This includes reading the process environment which potentially includes sensitive information, such as secrets. Furthermore, an attacker could leverage this vulnerability to use the Pulsar Functions Worker as a proxy to access the content of remote HTTP and HTTPS endpoint URLs. This could also be used to carry out denial of service attacks. This vulnerability also applies to the Pulsar Broker when it is configured with "functionsWorkerEnabled=true". This issue affects Apache Pulsar versions from 2.4.0 to 2.10.5, from 2.11.0 to 2.11.3, from 3.0.0 to 3.0.2, from 3.1.0 to 3.1.2, and 3.2.0. 2.10 Pulsar Function Worker users should upgrade to at least 2.10.6. 2.11 Pulsar Function Worker users should upgrade to at least 2.11.4. 3.0 Pulsar Function Worker users should upgrade to at least 3.0.3. 3.1 Pulsar Function Worker users should upgrade to at least 3.1.3. 3.2 Pulsar Function Worker users should upgrade to at least 3.2.1. Users operating versions prior to those listed above should upgrade to the aforementioned patched versions or newer versions. The updated versions of Pulsar Functions Worker will, by default, impose restrictions on the creation of functions using URLs. For users who rely on this functionality, the Function Worker configuration provides two configuration keys: "additionalEnabledConnectorUrlPatterns" and "additionalEnabledFunctionsUrlPatterns". These keys allow users to specify a set of URL patterns that are permitted, enabling the creation of functions using URLs that match the defined patterns. This approach ensures that the feature remains available to those who require it, while limiting the potential for unauthorized access and exploitation.	8.5	More Details
CVE-2024-27135	Improper input validation in the Pulsar Function Worker allows a malicious authenticated user to execute arbitrary Java code on the Pulsar Function worker, outside of the sandboxes designated for running user-provided functions. This vulnerability also applies to the Pulsar Broker when it is configured with "functionsWorkerEnabled=true". This issue affects Apache Pulsar versions from 2.4.0 to 2.10.5, from 2.11.0 to 2.11.3, from 3.0.0 to 3.0.2, from 3.1.0 to 3.1.2, and 3.2.0. 2.10 Pulsar Function Worker users should upgrade to at least 2.10.6. 2.11 Pulsar Function Worker users should upgrade to at least 2.11.4. 3.0 Pulsar Function Worker users should upgrade to at least 3.0.3. 3.1 Pulsar Function Worker users should upgrade to at least 3.1.3. 3.2 Pulsar Function Worker users should upgrade to at least 3.2.1. Users operating versions prior to those listed above should upgrade to the aforementioned patched versions or newer versions.	8.5	More Details
CVE-2024-27219	In tmu_set_pi of tmu.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2024-25988	In SAEMM_DiscloseGuti of SAEMM_RadioMessageCodec.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2024-25993	In tmu_reset_tmu_trip_counter of , there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2024-25817	Buffer Overflow vulnerability in eza before version 0.18.2, allows local attackers to execute arbitrary code via the .git/HEAD, .git/refs, and .git/objects components.	8.4	More Details
CVE-2023-33676	Sourcecodester Lost and Found Information System's Version 1.0 is vulnerable to unauthenticated SQL Injection at "?page=items/view&id=*" which can be escalated to the remote command execution.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25985	In bigo_unlocked_ioctl of bigo.c, there is a possible UAF due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2024-27204	In tmu_set_gov_active of tmu.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2024-27205	there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2024-22005	there is a possible Authentication Bypass due to improperly used crypto. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2024-27208	there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2024-27209	there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2024-27213	In BroadcastSystemMessage of servicemgr.cpp, there is a possible Remote Code Execution due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2024-27226	In tmu_config_gov_params of , there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2024-25999	An unauthenticated local attacker can perform a privilege escalation due to improper input validation in the OCPP agent service.	8.4	More Details
CVE-2024-27317	In Pulsar Functions Worker, authenticated users can upload functions in jar or nar files. These files, essentially zip files, are extracted by the Functions Worker. However, if a malicious file is uploaded, it could exploit a directory traversal vulnerability. This occurs when the filenames in the zip files, which aren't properly validated, contain special elements like "..", altering the directory path. This could allow an attacker to create or modify files outside of the designated extraction directory, potentially influencing system behavior. This vulnerability also applies to the Pulsar Broker when it is configured with "functionsWorkerEnabled=true". This issue affects Apache Pulsar versions from 2.4.0 to 2.10.5, from 2.11.0 to 2.11.3, from 3.0.0 to 3.0.2, from 3.1.0 to 3.1.2, and 3.2.0. 2.10 Pulsar Function Worker users should upgrade to at least 2.10.6. 2.11 Pulsar Function Worker users should upgrade to at least 2.11.4. 3.0 Pulsar Function Worker users should upgrade to at least 3.0.3. 3.1 Pulsar Function Worker users should upgrade to at least 3.1.3. 3.2 Pulsar Function Worker users should upgrade to at least 3.2.1. Users operating versions prior to those listed above should upgrade to the aforementioned patched versions or newer versions.	8.4	More Details
CVE-2024-27758	In RPyC before 6.0.0, when a server exposes a method that calls the attribute named __array__ for a client-provided netref (e.g., np.array(client_netref)), a remote attacker can craft a class that results in remote code execution.	8.4	More Details
CVE-2024-27220	In lpm_req_handler of , there is a possible out of bounds memory access due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27236	In aoc_unlocked_ioctl of aoc.c, there is a possible memory corruption due to type confusion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2022-34321	Improper Authentication vulnerability in Apache Pulsar Proxy allows an attacker to connect to the /proxy-stats endpoint without authentication. The vulnerable endpoint exposes detailed statistics about live connections, along with the capability to modify the logging level of proxied connections without requiring proper authentication credentials. This issue affects Apache Pulsar versions from 2.6.0 to 2.10.5, from 2.11.0 to 2.11.2, from 3.0.0 to 3.0.1, and 3.1.0. The known risks include exposing sensitive information such as connected client IP and unauthorized logging level manipulation which could lead to a denial-of-service condition by significantly increasing the proxy's logging overhead. When deployed via the Apache Pulsar Helm chart within Kubernetes environments, the actual client IP might not be revealed through the load balancer's default behavior, which typically obscures the original source IP addresses when externalTrafficPolicy is being configured to "Cluster" by default. The /proxy-stats endpoint contains topic level statistics, however, in the default configuration, the topic level statistics aren't known to be exposed. 2.10 Pulsar Proxy users should upgrade to at least 2.10.6. 2.11 Pulsar Proxy users should upgrade to at least 2.11.3. 3.0 Pulsar Proxy users should upgrade to at least 3.0.2. 3.1 Pulsar Proxy users should upgrade to at least 3.1.1. Users operating versions prior to those listed above should upgrade to the aforementioned patched versions or newer versions. Additionally, it's imperative to recognize that the Apache Pulsar Proxy is not intended for direct exposure to the internet. The architectural design of Pulsar Proxy assumes that it will operate within a secured network environment, safeguarded by appropriate perimeter defenses.	8.2	More Details
CVE-2024-20337	A vulnerability in the SAML authentication process of Cisco Secure Client could allow an unauthenticated, remote attacker to conduct a carriage return line feed (CRLF) injection attack against a user. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link while establishing a VPN session. A successful exploit could allow the attacker to execute arbitrary script code in the browser or access sensitive, browser-based information, including a valid SAML token. The attacker could then use the token to establish a remote access VPN session with the privileges of the affected user. Individual hosts and services behind the VPN headend would still need additional credentials for successful access.	8.2	More Details
CVE-2023-5410	A potential security vulnerability has been reported in the system BIOS of certain HP PC products, which might allow memory tampering. HP is releasing mitigation for the potential vulnerability.	8.2	More Details
CVE-2024-1220	A stack-based buffer overflow in the built-in web server in Moxa NPort W2150A/W2250A Series firmware version 2.3 and prior allows a remote attacker to exploit the vulnerability by sending crafted payload to the web service. Successful exploitation of the vulnerability could result in denial of service.	8.2	More Details
CVE-2024-1170	The Post Form – Registration Form – Profile Form for User Profiles – Frontend Content Forms for User Submissions (UGC) plugin for WordPress is vulnerable to unauthorized media file deletion due to a missing capability check on the handle_deleted_media function in all versions up to, and including, 2.8.7. This makes it possible for unauthenticated attackers to delete arbitrary media files.	8.2	More Details
CVE-2024-26566	An issue in Cute Http File Server v.3.1 allows a remote attacker to escalate privileges via the password verification component.	8.2	More Details
CVE-2023-42790	A stack-based buffer overflow in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27289	pgx is a PostgreSQL driver and toolkit for Go. Prior to version 4.18.2, SQL injection can occur when all of the following conditions are met: the non-default simple protocol is used; a placeholder for a numeric value must be immediately preceded by a minus; there must be a second placeholder for a string value after the first placeholder; both must be on the same line; and both parameter values must be user-controlled. The problem is resolved in v4.18.2. As a workaround, do not use the simple protocol or do not place a minus directly before a placeholder.	8.1	More Details
CVE-2024-21407	Windows Hyper-V Remote Code Execution Vulnerability	8.1	More Details
CVE-2024-1725	A flaw was found in the kubevirt-csi component of OpenShift Virtualization's Hosted Control Plane (HCP). This issue could allow an authenticated attacker to gain access to the root HCP worker node's volume by creating a custom Persistent Volume that matches the name of a worker node.	8.1	More Details
CVE-2024-22752	Insecure permissions issue in EaseUS MobiMover 6.0.5 Build 21620 allows attackers to gain escalated privileges via use of crafted executable launched from the application installation directory.	8.1	More Details
CVE-2022-46497	Hospital Management System 1.0 was discovered to contain a SQL injection vulnerability via the pat_number parameter at his_doc_view_single_patien.php.	8.1	More Details
CVE-2023-36554	A improper access control in Fortinet FortiManager version 7.4.0, version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.10, version 6.4.0 through 6.4.13, 6.2 all versions allows attacker to execute unauthorized code or commands via specially crafted HTTP requests.	8.1	More Details
CVE-2024-28114	Peering Manager is a BGP session management tool. There is a Server Side Template Injection vulnerability that leads to Remote Code Execution in Peering Manager <=1.8.2. As a result arbitrary commands can be executed on the operating system that is running Peering Manager. This issue has been addressed in version 1.8.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.1	More Details
CVE-2024-2338	PostgreSQL Anonymizer v1.2 contains a SQL injection vulnerability that allows a user who owns a table to elevate to superuser when dynamic masking is enabled. PostgreSQL Anonymizer enables users to set security labels on tables to mask specified columns. There is a flaw that allows complex expressions to be provided as a value. This expression is then later used as it to create the masked views leading to SQL Injection. If dynamic masking is enabled, this will lead to privilege escalation to superuser after the label is created. Users that don't own a table, especially masked users cannot exploit this vulnerability. The problem is resolved in v1.3.	8.0	More Details
CVE-2024-28157	Jenkins GitBucket Plugin 0.8 and earlier does not sanitize Gitbucket URLs on build views, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to configure jobs.	8.0	More Details
CVE-2024-2339	PostgreSQL Anonymizer v1.2 contains a vulnerability that allows a user who owns a table to elevate to superuser. A user can define a masking function for a column and place malicious code in that function. When a privileged user applies the masking rules using the static masking or the anonymous dump method, the malicious code is executed and can grant escalated privileges to the malicious user. PostgreSQL Anonymizer v1.2 does provide a protection against this risk with the restrict_to_trusted_schemas option, but that protection is incomplete. Users that don't own a table, especially masked users cannot exploit this vulnerability. The problem is resolved in v1.3.	8.0	More Details
CVE-2024-25951	A command injection vulnerability exists in local RACADM. A malicious authenticated user could gain control of the underlying operating system.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23112	An authorization bypass through user-controlled key vulnerability [CWE-639] in FortiOS version 7.4.0 through 7.4.1, 7.2.0 through 7.2.6, 7.0.1 through 7.0.13, 6.4.7 through 6.4.14, and FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14 SSL-VPN may allow an authenticated attacker to gain access to another user's bookmark via URL manipulation.	8.0	More Details
CVE-2024-28338	A login bypass in TOTOLINK A8000RU V7.1cu.643_B20200521 allows attackers to login to Administrator accounts via providing a crafted session cookie.	8.0	More Details
CVE-2024-25992	In tmu_tz_control of tmu.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-21805	Improper access control vulnerability exists in the specific folder of SKYSEA Client View versions from Ver.16.100 prior to Ver.19.2. If this vulnerability is exploited, an arbitrary file may be placed in the specific folder by a user who can log in to the PC where the product's Windows client is installed. In case the file is a specially crafted DLL file, arbitrary code may be executed with SYSTEM privilege.	7.8	More Details
CVE-2024-23611	An out of bounds write due to a missing bounds check in LabVIEW may result in remote code execution. Successful exploitation requires an attacker to provide a user with a specially crafted VI. This vulnerability affects LabVIEW 2024 Q1 and prior versions.	7.8	More Details
CVE-2024-23268	An injection issue was addressed with improved input validation. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to elevate privileges.	7.8	More Details
CVE-2024-23610	An out of bounds write due to a missing bounds check in LabVIEW may result in remote code execution. Successful exploitation requires an attacker to provide a user with a specially crafted VI. This vulnerability affects LabVIEW 2024 Q1 and prior versions.	7.8	More Details
CVE-2024-23270	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.7.4, macOS Ventura 13.6.5, macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4, tvOS 17.4. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2024-23609	An improper error handling vulnerability in LabVIEW may result in remote code execution. Successful exploitation requires an attacker to provide a user with a specially crafted VI. This vulnerability affects LabVIEW 2024 Q1 and prior versions.	7.8	More Details
CVE-2024-23608	An out of bounds write due to a missing bounds check in LabVIEW may result in remote code execution. Successful exploitation requires an attacker to provide a user with a specially crafted VI. This vulnerability affects LabVIEW 2024 Q1 and prior versions.	7.8	More Details
CVE-2024-26002	An improper input validation in the Qualcom plctool allows a local attacker with low privileges to gain root access by changing the ownership of specific files.	7.8	More Details
CVE-2024-23274	An injection issue was addressed with improved input validation. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to elevate privileges.	7.8	More Details
CVE-2024-23276	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to elevate privileges.	7.8	More Details
CVE-2024-23265	A memory corruption vulnerability was addressed with improved locking. This issue is fixed in macOS Monterey 12.7.4, macOS Ventura 13.6.5, macOS Sonoma 14.4, visionOS 1.1, iOS 17.4 and iPadOS 17.4, watchOS 10.4, iOS 16.7.6 and iPadOS 16.7.6, tvOS 17.4. An app may be able to cause unexpected system termination or write kernel memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23286	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.7.4, macOS Ventura 13.6.5, macOS Sonoma 14.4, visionOS 1.1, iOS 17.4 and iPadOS 17.4, watchOS 10.4, iOS 16.7.6 and iPadOS 16.7.6, tvOS 17.4. Processing an image may lead to arbitrary code execution.	7.8	More Details
CVE-2024-23288	This issue was addressed by removing the vulnerable code. This issue is fixed in tvOS 17.4, iOS 17.4 and iPadOS 17.4, macOS Sonoma 14.4, watchOS 10.4. An app may be able to elevate privileges.	7.8	More Details
CVE-2024-23294	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14.4. Processing malicious input may lead to code execution.	7.8	More Details
CVE-2024-23612	An improper error handling vulnerability in LabVIEW may result in remote code execution. Successful exploitation requires an attacker to provide a user with a specially crafted VI. This vulnerability affects LabVIEW 2024 Q1 and prior versions.	7.8	More Details
CVE-2024-0046	In installExistingPackageAsUser of InstallPackageHelper.java, there is a possible carrier restriction bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-27233	In ppcfw_init_secpolicy of ppcfw.c, there is a possible permission bypass due to uninitialized data. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-25986	In ppmp_unprotect_buf of drm_fw.c, there is a possible compromise of protected memory due to a logic error in the code. This could lead to local escalation of privilege to TEE with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-22008	In config_gov_time_windows of tmu.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-23233	This issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4. Entitlements and privacy permissions granted to this app may be used by a malicious app.	7.8	More Details
CVE-2024-26619	In the Linux kernel, the following vulnerability has been resolved: riscv: Fix module loading free order Reverse order of kfree calls to resolve use-after-free error.	7.8	More Details
CVE-2024-26610	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: fix a memory corruption iwl_fw_ini_trigger_tlv::data is a pointer to a __le32, which means that if we copy to iwl_fw_ini_trigger_tlv::data + offset while offset is in bytes, we'll write past the buffer.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26608	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix global oob in ksmbd_nl_policy Similar to a reported issue (check the commit b33fb5b801c6 ("net: qualcomm: rmnet: fix global oob in rmnet_policy"), my local fuzzer finds another global out-of-bounds read for policy ksmbd_nl_policy. See bug trace below: == BUG: KASAN: global-out-of-bounds in validate_nla lib/nlattr.c:386 [inline] BUG: KASAN: global-out-of-bounds in __nla_validate_parse+0x24af/0x2750 lib/nlattr.c:600 Read of size 1 at addr ffffffff8f24b100 by task syz-executor.1/62810 CPU: 0 PID: 62810 Comm: syz-executor.1 Tainted: G N 6.1.0 #3 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.13.0-1ubuntu1.1 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x8b/0xb3 lib/dump_stack.c:106 print_address_description mm/kasan/report.c:284 [inline] print_report+0x172/0x475 mm/kasan/report.c:395 kasan_report+0xbb/0x1c0 mm/kasan/report.c:495 validate_nla lib/nlattr.c:386 [inline] __nla_validate_parse+0x24af/0x2750 lib/nlattr.c:600 __nla_parse+0x3e/0x50 lib/nlattr.c:697 __nlmsg_parse include/net/netlink.h:748 [inline] genl_family_rcv_msg_attrs_parse.constprop.0+0x1b0/0x290 net/netlink/genetlink.c:565 genl_family_rcv_msg_doit+0xda/0x330 net/netlink/genetlink.c:734 genl_family_rcv_msg net/netlink/genetlink.c:833 [inline] genl_rcv_msg+0x441/0x780 net/netlink/genetlink.c:850 netlink_rcv_skb+0x14f/0x410 net/netlink/af_netlink.c:2540 genl_rcv+0x24/0x40 net/netlink/genetlink.c:861 netlink_unicast_kernel net/netlink/af_netlink.c:1319 [inline] netlink_unicast+0x54e/0x800 net/netlink/af_netlink.c:1345 netlink_sendmsg+0x930/0xe50 net/netlink/af_netlink.c:1921 sock_sendmsg_nosec net/socket.c:714 [inline] sock_sendmsg+0x154/0x190 net/socket.c:734 ____sys_sendmsg+0x6df/0x840 net/socket.c:2482 ___sys_sendmsg+0x110/0x1b0 net/socket.c:2536 __sys_sendmsg+0xf3/0x1c0 net/socket.c:2565 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x3b/0x90 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd RIP: 0033:0x7fdd66a8f359 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 f1 19 00 00 90 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 b8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007fdd65e00168 EFLAGS: 00000246 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 00007fdd66bbcf80 RCX: 00007fdd66a8f359 RDX: 0000000000000000 RSI: 0000000020000500 RDI: 0000000000000003 RBP: 00007fdd66ada493 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 00007ffc84b81aff R14: 00007fdd65e00300 R15: 0000000000022000 </TASK> The buggy address belongs to the variable: ksmbd_nl_policy+0x100/0xa80 The buggy address belongs to the physical page: page:0000000034f47940 refcount:1 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x1ccc4b flags: 0x200000000001000(reservedlnode=0lzone=2) raw: 0200000000001000 ffffea00073312c8 ffffea00073312c8 0000000000000000 raw: 0000000000000000 0000000000000000 00000001ffffffff 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffffffff8f24b000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ffffffff8f24b080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 >ffffffff8f24b100: f9 f9 f9 f9 00 00 f9 f9 f9 f9 f9 f9 00 00 07 f9 ^ ffffffff8f24b180: f9 f9 f9 f9 00 05 f9 f9 f9 f9 f9 f9 00 00 00 05 ffffffff8f24b200: f9 f9 f9 f9 00 00 03 f9 f9 f9 f9 f9 00 00 04 f9 == To fix it, add a placeholder named __KSMBD_EVENT_MAX and let KSMBD_EVENT_MAX to be its original value - 1 according to what other netlink families do. Also change two sites that refer the KSMBD_EVENT_MAX to correct value.	7.8	More Details
CVE-2024-23244	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4. An app from a standard user account may be able to escalate privilege after admin user login.	7.8	More Details
CVE-2024-23247	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. Processing a file may lead to unexpected app termination or arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52491	In the Linux kernel, the following vulnerability has been resolved: media: mtk-jpeg: Fix use after free bug due to error path handling in mtk_jpeg_dec_device_run In mtk_jpeg_probe, &jpeg->job_timeout_work is bound with mtk_jpeg_job_timeout_work. In mtk_jpeg_dec_device_run, if error happens in mtk_jpeg_set_dec_dst, it will finally start the worker while mark the job as finished by invoking v4l2_m2m_job_finish. There are two methods to trigger the bug. If we remove the module, it which will call mtk_jpeg_remove to make cleanup. The possible sequence is as follows, which will cause a use-after-free bug. CPU0 CPU1 mtk_jpeg_dec_... | start worker | |mtk_jpeg_job_timeout_work mtk_jpeg_remove | v4l2_m2m_release | kfree(m2m_dev); | | v4l2_m2m_get_curr_priv | m2m_dev->curr_ctx //use If we close the file descriptor, which will call mtk_jpeg_release, it will have a similar sequence. Fix this bug by starting timeout worker only if started jpegdec worker successfully. Then v4l2_m2m_job_finish will only be called in either mtk_jpeg_job_timeout_work or mtk_jpeg_dec_device_run.	7.8	More Details
CVE-2024-27210	In policy_check of fvp.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-27212	In init_data of , there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-1696	In Santesoft Sante FFT Imaging versions 1.4.1 and prior once a user opens a malicious DCM file on affected FFT Imaging installations, a local attacker could perform an out-of-bounds write, which could allow for arbitrary code execution.	7.8	More Details
CVE-2024-0051	In onQueueFilled of SoftMPEG4.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-0050	In getConfig of SoftVideoDecoderOMXComponent.cpp, there is a possible out of bounds write due to a missing validation check. This could lead to a local non-security issue with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-27221	In update_policy_data of , there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-23258	An out-of-bounds read was addressed with improved input validation. This issue is fixed in visionOS 1.1, macOS Sonoma 14.4. Processing an image may lead to arbitrary code execution.	7.8	More Details
CVE-2024-27222	In onSkipButtonClick of FaceEnrollFoldPage.java, there is a possible way to access the file the app cannot access due to Intent Redirect GRANT_URI_PERMISSIONS Attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-0049	In multiple locations, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-0048	In Session of AccountManagerService.java, there is a possible method to retain foreground service privileges due to incorrect handling of null responses. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-27224	In strncpy of strncpy.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26616	In the Linux kernel, the following vulnerability has been resolved: btrfs: scrub: avoid use-after-free when chunk length is not 64K aligned [BUG] There is a bug report that, on a ext4-converted btrfs, scrub leads to various problems, including: - "unable to find chunk map" errors BTRFS info (device vdb): scrub: started on devid 1 BTRFS critical (device vdb): unable to find chunk map for logical 2214744064 length 4096 BTRFS critical (device vdb): unable to find chunk map for logical 2214744064 length 45056 This would lead to unrepairable errors. - Use-after-free KASAN reports: == BUG: KASAN: slab-use-after-free in __blk_rq_map_sg+0x18f/0x7c0 Read of size 8 at addr ffff8881013c9040 by task btrfs/909 CPU: 0 PID: 909 Comm: btrfs Not tainted 6.7.0-x64v3-dbg #11 c50636e9419a8354555555245df535e380563b2b Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 2023.11-2 12/24/2023 Call Trace: <TASK> dump_stack_lvl+0x43/0x60 print_report+0xcf/0x640 kasan_report+0xa6/0xd0 __blk_rq_map_sg+0x18f/0x7c0 virtblk_prep_rq.isra.0+0x215/0x6a0 [virtio_blk 19a65eeee9ae6fcf02edfad39bb9ddee07dcdaff] virtio_queue_rqs+0xc4/0x310 [virtio_blk 19a65eeee9ae6fcf02edfad39bb9ddee07dcdaff] blk_mq_flush_plug_list.part.0+0x780/0x860 __blk_flush_plug+0x1ba/0x220 blk_finish_plug+0x3b/0x60 submit_initial_group_read+0x10a/0x290 [btrfs e57987a360bed82fe8756dcd3e0de5406ccfe965] flush_scrub_stripes+0x38e/0x430 [btrfs e57987a360bed82fe8756dcd3e0de5406ccfe965] scrub_stripe+0x82a/0xae0 [btrfs e57987a360bed82fe8756dcd3e0de5406ccfe965] scrub_chunk+0x178/0x200 [btrfs e57987a360bed82fe8756dcd3e0de5406ccfe965] scrub_enumerate_chunks+0x4bc/0xa30 [btrfs e57987a360bed82fe8756dcd3e0de5406ccfe965] btrfs_scrub_dev+0x398/0x810 [btrfs e57987a360bed82fe8756dcd3e0de5406ccfe965] btrfs_ioctl+0x4b9/0x3020 [btrfs e57987a360bed82fe8756dcd3e0de5406ccfe965] __x64_sys_ioctl+0xbd/0x100 do_syscall_64+0x5d/0xe0 entry_SYSCALL_64_after_hwframe+0x63/0x6b RIP: 0033:0x7f47e5e0952b - Crash, mostly due to above use-after-free [CAUSE] The converted fs has the following data chunk layout: item 2 key (FIRST_CHUNK_TREE CHUNK_ITEM 2214658048) itemoff 16025 itemsize 80 length 86016 owner 2 stripe_len 65536 type DATA|single For above logical bytenr 2214744064, it's at the chunk end (2214658048 + 86016 = 2214744064). This means btrfs_submit_bio() would split the bio, and trigger endio function for both of the two halves. However scrub_submit_initial_read() would only expect the endio function to be called once, not any more. This means the first endio function would already free the bbio::bio, leaving the bvec freed, thus the 2nd endio call would lead to use-after-free. [FIX] - Make sure scrub_read_endio() only updates bits in its range Since we may read less than 64K at the end of the chunk, we should not touch the bits beyond chunk boundary. - Make sure scrub_submit_initial_read() only to read the chunk range This is done by calculating the real number of sectors we need to read, and add sector-by-sector to the bio. Thankfully the scrub read repair path won't need extra fixes: - scrub_stripe_submit_repair_read() With above fixes, we won't update error bit for range beyond chunk, thus scrub_stripe_submit_repair_read() should never submit any read beyond the chunk.	7.8	More Details
CVE-2024-27907	A vulnerability has been identified in Simcenter Femap (All versions < V2306.0000). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted Catia MODEL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-22051)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52604	In the Linux kernel, the following vulnerability has been resolved: FS:JFS:UBSAN:array-index-out-of-bounds in dbAdjTree Syzkaller reported the following issue: UBSAN: array-index-out-of-bounds in fs/jfs/jfs_dmap.c:2867:6 index 196694 is out of range for type 's8[1365]' (aka 'signed char[1365]') CPU: 1 PID: 109 Comm: jfsCommit Not tainted 6.6.0-rc3-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/04/2023 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x1e7/0x2d0 lib/dump_stack.c:106 ubsan_epilogue lib/ubsan.c:217 [inline] __ubsan_handle_out_of_bounds+0x11c/0x150 lib/ubsan.c:348 dbAdjTree+0x474/0x4f0 fs/jfs/jfs_dmap.c:2867 dbJoin+0x210/0x2d0 fs/jfs/jfs_dmap.c:2834 dbFreeBits+0x4eb/0xda0 fs/jfs/jfs_dmap.c:2331 dbFreeDmap fs/jfs/jfs_dmap.c:2080 [inline] dbFree+0x343/0x650 fs/jfs/jfs_dmap.c:402 txFreeMap+0x798/0xd50 fs/jfs/jfs_txnmgr.c:2534 txUpdateMap+0x342/0x9e0 txLazyCommit fs/jfs/jfs_txnmgr.c:2664 [inline] jfs_lazycommit+0x47a/0xb70 fs/jfs/jfs_txnmgr.c:2732 kthread+0x2d3/0x370 kernel/kthread.c:388 ret_from_fork+0x48/0x80 arch/x86/kernel/process.c:147 ret_from_fork_asm+0x11/0x20 arch/x86/entry/entry_64.S:304 </TASK> == Kernel panic - not syncing: UBSAN: panic_on_warn set ... CPU: 1 PID: 109 Comm: jfsCommit Not tainted 6.6.0-rc3-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/04/2023 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x1e7/0x2d0 lib/dump_stack.c:106 panic+0x30f/0x770 kernel/panic.c:340 check_panic_on_warn+0x82/0xa0 kernel/panic.c:236 ubsan_epilogue lib/ubsan.c:223 [inline] __ubsan_handle_out_of_bounds+0x13c/0x150 lib/ubsan.c:348 dbAdjTree+0x474/0x4f0 fs/jfs/jfs_dmap.c:2867 dbJoin+0x210/0x2d0 fs/jfs/jfs_dmap.c:2834 dbFreeBits+0x4eb/0xda0 fs/jfs/jfs_dmap.c:2331 dbFreeDmap fs/jfs/jfs_dmap.c:2080 [inline] dbFree+0x343/0x650 fs/jfs/jfs_dmap.c:402 txFreeMap+0x798/0xd50 fs/jfs/jfs_txnmgr.c:2534 txUpdateMap+0x342/0x9e0 txLazyCommit fs/jfs/jfs_txnmgr.c:2664 [inline] jfs_lazycommit+0x47a/0xb70 fs/jfs/jfs_txnmgr.c:2732 kthread+0x2d3/0x370 kernel/kthread.c:388 ret_from_fork+0x48/0x80 arch/x86/kernel/process.c:147 ret_from_fork_asm+0x11/0x20 arch/x86/entry/entry_64.S:304 </TASK> Kernel Offset: disabled Rebooting in 86400 seconds.. The issue is caused when the value of lp becomes greater than CTLTREESIZE which is the max size of stree. Adding a simple check solves this issue. Dave: As the function returns a void, good error handling would require a more intrusive code reorganization, so I modified Osama's patch at use WARN_ON_ONCE for lack of a cleaner option. The patch is tested via syzbot.	7.8	More Details
CVE-2024-26199	Microsoft Office Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-21418	Software for Open Networking in the Cloud (SONiC) Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52603	In the Linux kernel, the following vulnerability has been resolved: UBSAN: array-index-out-of-bounds in dtSplitRoot Syzkaller reported the following issue: oop0: detected capacity change from 0 to 32768 UBSAN: array-index-out-of-bounds in fs/jfs/jfs_dtree.c:1971:9 index -2 is out of range for type 'struct dtslot [128]' CPU: 0 PID: 3613 Comm: syz-executor270 Not tainted 6.0.0-syzkaller-09423-g493ffd6605b2 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 09/22/2022 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x1b1/0x28e lib/dump_stack.c:106 ubsan_epilogue lib/ubsan.c:151 [inline] __ubsan_handle_out_of_bounds+0xdb/0x130 lib/ubsan.c:283 dtSplitRoot+0x8d8/0x1900 fs/jfs/jfs_dtree.c:1971 dtSplitUp fs/jfs/jfs_dtree.c:985 [inline] dtInsert+0x1189/0x6b80 fs/jfs/jfs_dtree.c:863 jfs_mkdir+0x757/0xb00 fs/jfs/namei.c:270 vfs_mkdir+0x3b3/0x590 fs/namei.c:4013 do_mkdirat+0x279/0x550 fs/namei.c:4038 __do_sys_mkdirat fs/namei.c:4053 [inline] __se_sys_mkdirat fs/namei.c:4051 [inline] __x64_sys_mkdirat+0x85/0x90 fs/namei.c:4051 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x3d/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd RIP: 0033:0x7fcdc0113fd9 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 c0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007ffeb8bc67d8 EFLAGS: 00000246 ORIG_RAX: 0000000000000102 RAX: ffffffffffffffda RBX: 0000000000000000 RCX: 00007fcdc0113fd9 RDX: 0000000000000000 RSI: 0000000020000340 RDI: 0000000000000003 RBP: 00007fcdc00d37a0 R08: 0000000000000000 R09: 00007fcdc00d37a0 R10: 00005555559a72c0 R11: 0000000000000246 R12: 00000000f8008000 R13: 0000000000000000 R14: 000838780000000f8 R15: 0000000000000000 </TASK> The issue is caused when the value of fsi becomes less than -1. The check to break the loop when fsi value becomes -1 is present but syzbot was able to produce value less than -1 which cause the error. This patch simply add the change for the values less than 0. The patch is tested via syzbot.	7.8	More Details
CVE-2024-24092	SQL Injection vulnerability in Code-projects.org Scholars Tracking System 1.0 allows attackers to run arbitrary code via login.php.	7.8	More Details
CVE-2024-21426	Microsoft SharePoint Server Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-21330	Open Management Infrastructure (OMI) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-23300	A use-after-free issue was addressed with improved memory management. This issue is fixed in GarageBand 10.4.11. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution.	7.8	More Details
CVE-2024-21431	Hypervisor-Protected Code Integrity (HVCI) Security Feature Bypass Vulnerability	7.8	More Details
CVE-2024-21434	Microsoft Windows SCSI Class System File Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-21436	Windows Installer Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-52591	In the Linux kernel, the following vulnerability has been resolved: reiserfs: Avoid touching renamed directory if parent does not change The VFS will not be locking moved directory if its parent does not change. Change reiserfs rename code to avoid touching renamed directory if its parent does not change as without locking that can corrupt the filesystem.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21442	Windows USB Print Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-52594	In the Linux kernel, the following vulnerability has been resolved: wifi: ath9k: Fix potential array-index-out-of-bounds read in ath9k_htc_txstatus() Fix an array-index-out-of-bounds read in ath9k_htc_txstatus(). The bug occurs when txs->cnt, data from a URB provided by a USB device, is bigger than the size of the array txs->txstatus, which is HTC_MAX_TX_STATUS. WARN_ON() already checks it, but there is no bug handling code after the check. Make the function return if that is the case. Found by a modified version of syzkaller. UBSAN: array-index-out-of-bounds in htc_drv_txrx.c index 13 is out of range for type '__wmi_event_txstatus [12]' Call Trace: ath9k_htc_txstatus ath9k_wmi_event_tasklet tasklet_action_common __do_softirq irq_exit_rxu sysvec_apic_timer_interrupt	7.8	More Details
CVE-2024-21446	NTFS Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-21437	Windows Graphics Component Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-1618	A search path or unquoted item vulnerability in Faronics Deep Freeze Server Standard, which affects versions 8.30.020.4627 and earlier. This vulnerability affects the DFServ.exe file. An attacker with local user privileges could exploit this vulnerability to replace the legitimate DFServ.exe service executable with a malicious file of the same name and located in a directory that has a higher priority than the legitimate directory. Thus, when the service starts, it will run the malicious file instead of the legitimate executable, allowing the attacker to execute arbitrary code, gain unauthorized access to the compromised system or stop the service from running.	7.8	More Details
CVE-2024-26176	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-25102	This vulnerability exists in AppSamvid software due to the usage of a weaker cryptographic algorithm (hash) SHA1 in user login component. An attacker with local administrative privileges could exploit this to obtain the password of AppSamvid on the targeted system. Successful exploitation of this vulnerability could allow the attacker to take complete control of the application on the targeted system.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52599	In the Linux kernel, the following vulnerability has been resolved: jfs: fix array-index-out-of-bounds in diNewExt [Syz report] UBSAN: array-index-out-of-bounds in fs/jfs/jfs_imap.c:2360:2 index -878706688 is out of range for type 'struct iagctl[128]' CPU: 1 PID: 5065 Comm: syz-executor282 Not tainted 6.7.0-rc4-syzkaller-00009-gbee0e7762ad2 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 11/10/2023 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x1e7/0x2d0 lib/dump_stack.c:106 ubsan_epilogue lib/ubsan.c:217 [inline] __ubsan_handle_out_of_bounds+0x11c/0x150 lib/ubsan.c:348 diNewExt+0x3cf3/0x4000 fs/jfs/jfs_imap.c:2360 diAllocExt fs/jfs/jfs_imap.c:1949 [inline] diAllocAG+0xbe8/0x1e50 fs/jfs/jfs_imap.c:1666 diAlloc+0x1d3/0x1760 fs/jfs/jfs_imap.c:1587 ialloc+0x8f/0x900 fs/jfs/jfs_inode.c:56 jfs_mkdir+0x1c5/0xb90 fs/jfs/namei.c:225 vfs_mkdir+0x2f1/0x4b0 fs/namei.c:4106 do_mkdirat+0x264/0x3a0 fs/namei.c:4129 __do_sys_mkdir fs/namei.c:4149 [inline] __se_sys_mkdir fs/namei.c:4147 [inline] __x64_sys_mkdir+0x6e/0x80 fs/namei.c:4147 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x45/0x110 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x63/0x6b RIP: 0033:0x7fcb7e6a0b57 Code: ff ff 77 07 31 c0 c3 0f 1f 40 00 48 c7 c2 b8 ff ff ff f7 d8 64 89 02 b8 ff ff ff ff c3 66 0f 1f 44 00 00 b8 53 00 00 00 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007ffd83023038 EFLAGS: 00000286 ORIG_RAX: 0000000000000053 RAX: ffffffffffffffda RBX: 00000000ffffffff RCX: 00007fcb7e6a0b57 RDX: 00000000000a1020 RSI: 00000000000001ff RDI: 0000000020000140 RBP: 0000000020000140 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000286 R12: 00007ffd830230d0 R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 [Analysis] When the agstart is too large, it can cause agno overflow. [Fix] After obtaining agno, if the value is invalid, exit the subsequent process. Modified the test from agno > MAXAG to agno >= MAXAG based on linux-next report by kernel test robot (Dan Carpenter).	7.8	More Details
CVE-2024-26182	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-52600	In the Linux kernel, the following vulnerability has been resolved: jfs: fix uaf in jfs_evict_inode When the execution of diMount(ipimap) fails, the object ipimap that has been released may be accessed in diFreeSpecial(). Asynchronous ipimap release occurs when rcu_core() calls jfs_free_node(). Therefore, when diMount(ipimap) fails, sbi->ipimap should not be initialized as ipimap.	7.8	More Details
CVE-2024-26178	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-52601	In the Linux kernel, the following vulnerability has been resolved: jfs: fix array-index-out-of-bounds in dbAdjTree Currently there is a bound check missing in the dbAdjTree while accessing the dmt_stree. To add the required check added the bool is_ctl which is required to determine the size as suggest in the following commit. https://lore.kernel.org/linux-kernel-mentees/f9475918-2186-49b8-b801-6f0f9e75f4fa@oracle.com/	7.8	More Details
CVE-2024-26173	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-52602	In the Linux kernel, the following vulnerability has been resolved: jfs: fix slab-out-of-bounds Read in dtSearch Currently while searching for current page in the sorted entry table of the page there is a out of bound access. Added a bound check to fix the error. Dave: Set return code to -EIO	7.8	More Details
CVE-2024-26170	Windows Composite Image File System (CimFS) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-26169	Windows Error Reporting Service Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27733	File Upload vulnerability in Byzro Network Smart s42 Management Platform v.S42 allows a local attacker to execute arbitrary code via the useratte/userattestation.php component.	7.7	More Details
CVE-2024-0199	An authorization bypass vulnerability was discovered in GitLab affecting versions 11.3 prior to 16.7.7, 16.7.6 prior to 16.8.4, and 16.8.3 prior to 16.9.2. An attacker could bypass CODEOWNERS by utilizing a crafted payload in an old feature branch to perform malicious actions.	7.7	More Details
CVE-2024-27211	In AtiHandleAPOMsgType of ati_Main.c, there is a possible OOB write due to a missing null check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.7	More Details
CVE-2024-28236	Vela is a Pipeline Automation (CI/CD) framework built on Linux container technology written in Golang. Vela pipelines can use variable substitution combined with insensitive fields like `parameters`, `image` and `entrypoint` to inject secrets into a plugin/image and — by using common substitution string manipulation — can bypass log masking and expose secrets without the use of the commands block. This unexpected behavior primarily impacts secrets restricted by the "no commands" option. This can lead to unintended use of the secret value, and increased risk of exposing the secret during image execution bypassing log masking. **To exploit this** the pipeline author must be supplying the secrets to a plugin that is designed in such a way that will print those parameters in logs. Plugin parameters are not designed for sensitive values and are often intentionally printed throughout execution for informational/debugging purposes. Parameters should therefore be treated as insensitive. While Vela provides secrets masking, secrets exposure is not entirely solved by the masking process. A docker image (plugin) can easily expose secrets if they are not handled properly, or altered in some way. There is a responsibility on the end-user to understand how values injected into a plugin are used. This is a risk that exists for many CICD systems (like GitHub Actions) that handle sensitive runtime variables. Rather, the greater risk is that users who restrict a secret to the "no commands" option and use image restriction can still have their secret value exposed via substitution tinkering, which turns the image and command restrictions into a false sense of security. This issue has been addressed in version 0.23.2. Users are advised to upgrade. Users unable to upgrade should not provide sensitive values to plugins that can potentially expose them, especially in `parameters` that are not intended to be used for sensitive values, ensure plugins (especially those that utilize shared secrets) follow best practices to avoid logging parameters that are expected to be sensitive, minimize secrets with `pull_request` events enabled, as this allows users to change pipeline configurations and pull in secrets to steps not typically part of the CI process, make use of the build approval setting, restricting builds from untrusted users, and limit use of shared secrets, as they are less restrictive to access by nature.	7.7	More Details
CVE-2024-21419	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	7.6	More Details
CVE-2024-22045	A vulnerability has been identified in SINEMA Remote Connect Client (All versions < V3.1 SP1). The product places sensitive information into files or directories that are accessible to actors who are allowed to have access to the files, but not to the sensitive information. This information is also available via the web interface of the product.	7.6	More Details
CVE-2024-27308	Mio is a Metal I/O library for Rust. When using named pipes on Windows, mio will under some circumstances return invalid tokens that correspond to named pipes that have already been deregistered from the mio registry. The impact of this vulnerability depends on how mio is used. For some applications, invalid tokens may be ignored or cause a warning or a crash. On the other hand, for applications that store pointers in the tokens, this vulnerability may result in a use-after-free. For users of Tokio, this vulnerability is serious and can result in a use-after-free in Tokio. The vulnerability is Windows-specific, and can only happen if you are using named pipes. Other IO resources are not affected. This vulnerability has been fixed in mio v0.8.11. All versions of mio between v0.7.2 and v0.8.10 are vulnerable. Tokio is vulnerable when you are using a vulnerable version of mio AND you are using at least Tokio v1.30.0. Versions of Tokio prior to v1.30.0 will ignore invalid tokens, so they are not vulnerable. Vulnerable libraries that use mio can work around this issue by detecting and ignoring invalid tokens.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48703	RobotsAndPencils go-saml, a SAML client library written in Go, contains an authentication bypass vulnerability in all known versions. This is due to how the `xmlsec1` command line tool is called internally to verify the signature of SAML assertions. When `xmlsec1` is used without defining the enabled key data, the origin of the public key for the signature verification is, unfortunately, not restricted. That means an attacker can sign the SAML assertions themselves and provide the required public key (e.g. an RSA key) directly embedded in the SAML token. Projects still using RobotsAndPencils/go-saml should move to another SAML library or alternatively remove support for SAML from their projects. The vulnerability can likely temporarily be fixed by forking the go-saml project and adding the command line argument `--enabled-key-data` and specifying a value such as `x509` or `raw-x509-cert` when calling the `xmlsec1` binary in the verify function. Please note that this workaround must be carefully tested before it can be used.	7.5	More Details
CVE-2024-21421	Azure SDK Spoofing Vulnerability	7.5	More Details
CVE-2019-6268	RAD SecFlow-2 devices with Hardware 0202, Firmware 4.1.01.63, and U-Boot 2010.12 allow URIs beginning with /.. for Directory Traversal, as demonstrated by reading /etc/shadow.	7.5	More Details
CVE-2024-27206	there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	7.5	More Details
CVE-2024-21427	Windows Kerberos Security Feature Bypass Vulnerability	7.5	More Details
CVE-2024-24765	CasaOS-UserService provides user management functionalities to CasaOS. Prior to version 0.4.7, path filtering of the URL for user avatar image files was not strict, making it possible to get any file on the system. This could allow an unauthorized actor to access, for example, the CasaOS user database, and possibly obtain system root privileges. Version 0.4.7 fixes this issue.	7.5	More Details
CVE-2024-26190	Microsoft QUIC Denial of Service Vulnerability	7.5	More Details
CVE-2024-24761	Galette is a membership management web application for non profit organizations. Starting in version 1.0.0 and prior to version 1.0.2, public pages are per default restricted to only administrators and staff members. From configuration, it is possible to restrict to up-to-date members or to everyone. Version 1.0.2 fixes this issue.	7.5	More Details
CVE-2024-28340	An information leak in the currentsetting.htm component of Netgear CBR40 2.5.0.28, Netgear CBK40 2.5.0.28, and Netgear CBK43 2.5.0.28 allows attackers to obtain sensitive information without any authentication required.	7.5	More Details
CVE-2024-21438	Microsoft AllJoyn API Denial of Service Vulnerability	7.5	More Details
CVE-2024-26204	Outlook for Android Information Disclosure Vulnerability	7.5	More Details
CVE-2024-28110	Go SDK for CloudEvents is the official CloudEvents SDK to integrate applications with CloudEvents. Prior to version 2.15.2, using cloudevents.WithRoundTripper to create a cloudevents.Client with an authenticated http.RoundTripper causes the go-sdk to leak credentials to arbitrary endpoints. When the transport is populated with an authenticated transport, then http.DefaultClient is modified with the authenticated transport and will start to send Authorization tokens to any endpoint it is used to contact. Version 2.15.2 patches this issue.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27917	Shopware is an open commerce platform based on Symfony Framework and Vue. The Symfony Session Handler pops the Session Cookie and assigns it to the Response. Since Shopware 6.5.8.0, the 404 pages are cached to improve the performance of 404 pages. So the cached Response which contains a Session Cookie when the Browser accessing the 404 page, has no cookies yet. The Symfony Session Handler is in use, when no explicit Session configuration has been done. When Redis is in use for Sessions using the PHP Redis extension, this exploiting code is not used. Shopware version 6.5.8.7 contains a patch for this issue. As a workaround, use Redis for Sessions, as this does not trigger the exploit code.	7.5	More Details
CVE-2023-49341	An issue was discovered in Newland Nquire 1000 Interactive Kiosk version NQ1000-II_G_V1.00.011, allows remote attackers to obtain sensitive information via cleartext credential storage in backup.htm component.	7.5	More Details
CVE-2024-26004	An unauthenticated remote attacker can DoS a control agent due to access of a uninitialized pointer which may prevent or disrupt the charging functionality.	7.5	More Details
CVE-2024-28215	nGrinder before 3.5.9 allows an attacker to create or update webhook configuration due to lack of access control, which could be the cause of information disclosure and limited Server-Side Request Forgery.	7.5	More Details
CVE-2024-1169	The Post Form – Registration Form – Profile Form for User Profiles – Frontend Content Forms for User Submissions (UGC) plugin for WordPress is vulnerable to unauthorized media upload due to a missing capability check on the buddyforms_upload_handle_dropped_media function in all versions up to, and including, 2.8.7. This makes it possible for unauthenticated attackers to upload media files.	7.5	More Details
CVE-2024-22040	A vulnerability has been identified in Cerberus PRO EN Engineering Tool (All versions), Cerberus PRO EN Fire Panel FC72x IP6 (All versions), Cerberus PRO EN Fire Panel FC72x IP7 (All versions), Cerberus PRO EN Fire Panel FC72x IP8 (All versions < IP8 SR4), Cerberus PRO EN X200 Cloud Distribution IP7 (All versions), Cerberus PRO EN X200 Cloud Distribution IP8 (All versions < V4.3.5618), Cerberus PRO EN X300 Cloud Distribution IP7 (All versions), Cerberus PRO EN X300 Cloud Distribution IP8 (All versions < V4.3.5617), Cerberus PRO UL Compact Panel FC922/924 (All versions < MP4), Cerberus PRO UL Engineering Tool (All versions < MP4), Cerberus PRO UL X300 Cloud Distribution (All versions < V4.3.0001), Desigo Fire Safety UL Compact Panel FC2025/2050 (All versions < MP4), Desigo Fire Safety UL Engineering Tool (All versions < MP4), Desigo Fire Safety UL X300 Cloud Distribution (All versions < V4.3.0001), Sinteso FS20 EN Engineering Tool (All versions), Sinteso FS20 EN Fire Panel FC20 MP6 (All versions), Sinteso FS20 EN Fire Panel FC20 MP7 (All versions), Sinteso FS20 EN Fire Panel FC20 MP8 (All versions < MP8 SR4), Sinteso FS20 EN X200 Cloud Distribution MP7 (All versions), Sinteso FS20 EN X200 Cloud Distribution MP8 (All versions < V4.3.5618), Sinteso FS20 EN X300 Cloud Distribution MP7 (All versions), Sinteso FS20 EN X300 Cloud Distribution MP8 (All versions < V4.3.5617), Sinteso Mobile (All versions). The network communication library in affected systems insufficiently validates HMAC values which might result in a buffer overread. This could allow an unauthenticated remote attacker to crash the network service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22041	A vulnerability has been identified in Cerberus PRO EN Engineering Tool (All versions), Cerberus PRO EN Fire Panel FC72x IP6 (All versions), Cerberus PRO EN Fire Panel FC72x IP7 (All versions), Cerberus PRO EN Fire Panel FC72x IP8 (All versions < IP8 SR4), Cerberus PRO EN X200 Cloud Distribution IP7 (All versions), Cerberus PRO EN X200 Cloud Distribution IP8 (All versions < V4.3.5618), Cerberus PRO EN X300 Cloud Distribution IP7 (All versions), Cerberus PRO EN X300 Cloud Distribution IP8 (All versions < V4.3.5617), Cerberus PRO UL Compact Panel FC922/924 (All versions < MP4), Cerberus PRO UL Engineering Tool (All versions < MP4), Cerberus PRO UL X300 Cloud Distribution (All versions < V4.3.0001), Desigo Fire Safety UL Compact Panel FC2025/2050 (All versions < MP4), Desigo Fire Safety UL Engineering Tool (All versions < MP4), Desigo Fire Safety UL X300 Cloud Distribution (All versions < V4.3.0001), Sinteso FS20 EN Engineering Tool (All versions), Sinteso FS20 EN Fire Panel FC20 MP6 (All versions), Sinteso FS20 EN Fire Panel FC20 MP7 (All versions), Sinteso FS20 EN Fire Panel FC20 MP8 (All versions < MP8 SR4), Sinteso FS20 EN X200 Cloud Distribution MP7 (All versions), Sinteso FS20 EN X200 Cloud Distribution MP8 (All versions < V4.3.5618), Sinteso FS20 EN X300 Cloud Distribution MP7 (All versions), Sinteso FS20 EN X300 Cloud Distribution MP8 (All versions < V4.3.5617), Sinteso Mobile (All versions). The network communication library in affected systems improperly handles memory buffers when parsing X.509 certificates. This could allow an unauthenticated remote attacker to crash the network service.	7.5	More Details
CVE-2024-26003	An unauthenticated remote attacker can DoS the control agent due to a out-of-bounds read which may prevent or disrupt the charging functionality.	7.5	More Details
CVE-2024-28754	RaspAP (aka raspap-webgui) through 3.0.9 allows remote attackers to cause a persistent denial of service (bricking) via a crafted request.	7.5	More Details
CVE-2023-47415	Cypress Solutions CTM-200 v2.7.1.5600 and below was discovered to contain an OS command injection vulnerability via the cli_text parameter.	7.5	More Details
CVE-2024-22044	A vulnerability has been identified in SENTRON 3KC ATC6 Expansion Module Ethernet (3KC9000-8TL75) (All versions). Affected devices expose an unused, unstable http service at port 80/tcp on the Modbus-TCP Ethernet. This could allow an attacker on the same Modbus network to create a denial of service condition that forces the device to reboot.	7.5	More Details
CVE-2024-1931	NLnet Labs Unbound version 1.18.0 up to and including version 1.19.1 contain a vulnerability that can cause denial of service by a certain code path that can lead to an infinite loop. Unbound 1.18.0 introduced a feature that removes EDE records from responses with size higher than the client's advertised buffer size. Before removing all the EDE records however, it would try to see if trimming the extra text fields on those records would result in an acceptable size while still retaining the EDE codes. Due to an unchecked condition, the code that trims the text of the EDE records could loop indefinitely. This happens when Unbound would reply with attached EDE information on a positive reply and the client's buffer size is smaller than the needed space to include EDE records. The vulnerability can only be triggered when the 'ede: yes' option is used; non default configuration. From version 1.19.2 on, the code is fixed to avoid looping indefinitely.	7.5	More Details
CVE-2022-46070	GV-ASManager V6.0.1.0 contains a Local File Inclusion vulnerability in GeoWebServer via Path.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28197	Zitadel is an open source identity management system. Zitadel uses a cookie to identify the user agent (browser) and its user sessions. Although the cookie was handled according to best practices, it was accessible on subdomains of the ZITADEL instance. An attacker could take advantage of this and provide a malicious link hosted on the subdomain to the user to gain access to the victim's account in certain scenarios. A possible victim would need to login through the malicious link for this exploit to work. If the possible victim already had the cookie present, the attack would not succeed. The attack would further only be possible if there was an initial vulnerability on the subdomain. This could either be the attacker being able to control DNS or a XSS vulnerability in an application hosted on a subdomain. Versions 2.46.0, 2.45.1, and 2.44.3 have been patched. Zitadel recommends upgrading to the latest versions available in due course. Note that applying the patch will invalidate the current cookie and thus users will need to start a new session and existing sessions (user selection) will be empty. For self-hosted environments unable to upgrade to a patched version, prevent setting the following cookie name on subdomains of your Zitadel instance (e.g. within your WAF): `__Secure-zitadel-useragent`.	7.5	More Details
CVE-2024-1226	The software does not neutralize or incorrectly neutralizes certain characters before the data is included in outgoing HTTP headers. The inclusion of invalidated data in an HTTP header allows an attacker to specify the full HTTP response represented by the browser. An attacker could control the response and craft attacks such as cross-site scripting and cache poisoning attacks.	7.5	More Details
CVE-2023-46717	An improper authentication vulnerability [CWE-287] in FortiOS versions 7.4.1 and below, versions 7.2.6 and below, and versions 7.0.12 and below when configured with FortiAuthenticator in HA may allow a readonly user to gain read-write access via successive login attempts.	7.5	More Details
CVE-2024-24375	SQL injection vulnerability in Jfinalcms v.5.0.0 allows a remote attacker to obtain sensitive information via /admin/admin name parameter.	7.5	More Details
CVE-2023-7072	The Post Grid Combo – 36+ Gutenberg Blocks plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.2.68 via the 'get_posts' REST API Endpoint. This makes it possible for unauthenticated attackers to extract sensitive data including full draft posts and password protected posts, as well as the password for password-protected posts.	7.5	More Details
CVE-2024-21392	.NET and Visual Studio Denial of Service Vulnerability	7.5	More Details
CVE-2023-49988	Hotel Booking Management v1.0 was discovered to contain a SQL injection vulnerability via the npss parameter at rooms.php.	7.5	More Details
CVE-2024-28184	WeasyPrint helps web developers to create PDF documents. Since version 61.0, there's a vulnerability which allows attaching content of arbitrary files and URLs to a generated PDF document, even if `url_fetcher` is configured to prevent access to files and URLs. This vulnerability has been patched in version 61.2.	7.4	More Details
CVE-2024-26001	An unauthenticated remote attacker can write memory out of bounds due to improper input validation in the MQTT stack. The brute force attack is not always successful because of memory randomization.	7.4	More Details
CVE-2024-1528	CMS Made Simple version 2.2.14, does not sufficiently encode user-controlled input, resulting in a Cross-Site Scripting (XSS) vulnerability through /admin/moduleinterface.php, in multiple parameters. This vulnerability could allow a remote attacker to send a specially crafted JavaScript payload to an authenticated user and partially hijack their browser session.	7.4	More Details
CVE-2024-1529	Vulnerability in CMS Made Simple 2.2.14, which does not sufficiently encode user-controlled input, resulting in a Cross-Site Scripting (XSS) vulnerability through /admin/adduser.php, in multiple parameters. This vulnerability could allow a remote attacker to send a specially crafted JavaScript payload to an authenticated user and partially take over their browser session.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2395	The Bulgarisation for WooCommerce plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.0.14. This is due to missing or incorrect nonce validation on several functions. This makes it possible for unauthenticated attackers to generate and delete labels via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	7.3	More Details
CVE-2024-21443	Windows Kernel Elevation of Privilege Vulnerability	7.3	More Details
CVE-2024-20338	A vulnerability in the ISE Posture (System Scan) module of Cisco Secure Client for Linux could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to the use of an uncontrolled search path element. An attacker could exploit this vulnerability by copying a malicious library file to a specific directory in the filesystem and persuading an administrator to restart a specific process. A successful exploit could allow the attacker to execute arbitrary code on an affected device with root privileges.	7.3	More Details
CVE-2024-28097	Calendar functionality in Schoolbox application before version 23.1.3 is vulnerable to stored cross-site scripting allowing authenticated attacker to perform security actions in the context of the affected users.	7.3	More Details
CVE-2024-26203	Azure Data Studio Elevation of Privilege Vulnerability	7.3	More Details
CVE-2024-2264	A vulnerability, which was classified as critical, has been found in keerti1924 PHP-MYSQL-User-Login-System 1.0. Affected by this issue is some unknown functionality of the file /login.php. The manipulation of the argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-256034 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2024-2282	A vulnerability was found in boyiddha Automated-Mess-Management-System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /index.php of the component Login Page. The manipulation of the argument useremail leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256049 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2024-28096	Class functionality in Schoolbox application before version 23.1.3 is vulnerable to stored cross-site scripting allowing authenticated attacker to perform security actions in the context of the affected users.	7.3	More Details
CVE-2024-25998	An unauthenticated remote attacker can perform a command injection in the OCPP Service with limited privileges due to improper input validation.	7.3	More Details
CVE-2024-27303	electron-builder is a solution to package and build a ready for distribution Electron, Proton Native app for macOS, Windows and Linux. A vulnerability that only affects eletron-builder prior to 24.13.2 in Windows, the NSIS installer makes a system call to open cmd.exe via NSExec in the `.nsh` installer script. NSExec by default searches the current directory of where the installer is located before searching `PATH`. This means that if an attacker can place a malicious executable file named cmd.exe in the same folder as the installer, the installer will run the malicious file. Version 24.13.2 fixes this issue. No known workaround exists. The code executes at the installer-level before the app is present on the system, so there's no way to check if it exists in a current installer.	7.3	More Details
CVE-2024-1302	Information exposure vulnerability in Badger Meter Monitool affecting versions up to 4.6.3 and earlier. A local attacker could change the application's file parameter to a log file obtaining all sensitive information such as database credentials.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26313	Archer Platform 6.x before 6.14 P2 HF2 (6.14.0.2.2) contains a stored cross-site scripting (XSS) vulnerability. A remote authenticated malicious Archer user could potentially exploit this to store malicious HTML or JavaScript code in a trusted application data store. When victim users access the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable application. 6.13.P3 HF1 (6.13.0.3.1) is also a fixed release.	7.3	More Details
CVE-2024-28095	News functionality in Schoolbox application before version 23.1.3 is vulnerable to stored cross-site scripting allowing authenticated attacker to perform security actions in the context of the affected users.	7.3	More Details
CVE-2024-1068	The 404 Solution WordPress plugin before 2.35.8 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admins.	7.2	More Details
CVE-2023-48725	A stack-based buffer overflow vulnerability exists in the JSON Parsing getblockschedule() functionality of Netgear RAX30 1.0.11.96 and 1.0.7.78. A specially crafted HTTP request can lead to code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	7.2	More Details
CVE-2024-0386	The weForms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Referer' HTTP header in all versions up to, and including, 1.6.21 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-2024-28187	SOY CMS is an open source CMS (content management system) that allows you to build blogs and online shops. SOY CMS versions prior to 3.14.2 are vulnerable to an OS Command Injection vulnerability within the file upload feature when accessed by an administrator. The vulnerability enables the execution of arbitrary OS commands through specially crafted file names containing a semicolon, affecting the jpegoptim functionality. This vulnerability has been patched in version 3.14.2. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.2	More Details
CVE-2023-42661	JFrog Artifactory prior to version 7.76.2 is vulnerable to Arbitrary File Write of untrusted data, which may lead to DoS or Remote Code Execution when a specially crafted series of requests is sent by an authenticated user. This is due to insufficient validation of artifacts.	7.2	More Details
CVE-2024-27121	Path traversal vulnerability exists in Machine Automation Controller NJ Series and Machine Automation Controller NX Series. An arbitrary file in the affected product may be accessed or arbitrary code may be executed by processing a specially crafted request sent from a remote attacker with an administrative privilege. As for the details of the affected product names/versions, see the information provided by the vendor under [References] section.	7.2	More Details
CVE-2024-23248	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.4. Processing a file may lead to a denial-of-service or potentially disclose memory contents.	7.1	More Details
CVE-2024-23249	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.4. Processing a file may lead to a denial-of-service or potentially disclose memory contents.	7.1	More Details
CVE-2024-1224	This vulnerability exists in USB Pratirodh due to the usage of a weaker cryptographic algorithm (hash) SHA1 in user login component. A local attacker with administrative privileges could exploit this vulnerability to obtain the password of USB Pratirodh on the targeted system. Successful exploitation of this vulnerability could allow the attacker to take control of the application and modify the access control of registered users or devices on the targeted system.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28186	FreeScout is an open source help desk and shared inbox built with PHP. A vulnerability has been identified in the Free Scout Application, which exposes SMTP server credentials used by an organization in the application to users of the application. This issue arises from the application storing complete stack traces of exceptions in its database. The sensitive information is then inadvertently disclosed to users via the `/conversation/ajax-html/send_log?folder_id=&thread_id={id}` endpoint. The stack trace reveals value of parameters, including the username and password, passed to the `Swift_Transport_Esmtp_Auth_LoginAuthenticator->authenticate()` function. Exploiting this vulnerability allows an attacker to gain unauthorized access to SMTP server credentials. With this sensitive information in hand, the attacker can potentially send unauthorized emails from the compromised SMTP server, posing a severe threat to the confidentiality and integrity of email communications. This could lead to targeted attacks on both the application users and the organization itself, compromising the security of email exchange servers. This issue has been addressed in version 1.8.124. Users are advised to upgrade. Users unable to upgrade should adopt the following measures: 1. Avoid Storing Complete Stack Traces, 2. Implement redaction mechanisms to filter and exclude sensitive information, and 3. Review and enhance the application's logging practices.	7.1	More Details
CVE-2024-23216	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to overwrite arbitrary files.	7.1	More Details
CVE-2024-25325	SQL injection vulnerability in Employee Management System v.1.0 allows a local attacker to obtain sensitive information via a crafted payload to the txtemail parameter in the login.php.	7.1	More Details
CVE-2024-22009	In init_data of , there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.1	More Details
CVE-2024-28199	phlex is an open source framework for building object-oriented views in Ruby. There is a potential cross-site scripting (XSS) vulnerability that can be exploited via maliciously crafted user data. This was due to improper case-sensitivity in the code that was meant to prevent these attacks. If you render an `<a>` tag with an `href` attribute set to a user-provided link, that link could potentially execute JavaScript when clicked by another user. If you splat user-provided attributes when rendering any HTML tag, malicious event attributes could be included in the output, executing JavaScript when the events are triggered by another user. Patches are available on RubyGems for all 1.x minor versions. Users are advised to upgrade. Users unable to upgrade should consider configuring a content security policy that does not allow `unsafe-inline`.	7.1	More Details
CVE-2024-21390	Microsoft Authenticator Elevation of Privilege Vulnerability	7.1	More Details
CVE-2024-21432	Windows Update Stack Elevation of Privilege Vulnerability	7.0	More Details
CVE-2024-21433	Windows Print Spooler Elevation of Privilege Vulnerability	7.0	More Details
CVE-2024-21445	Windows USB Print Driver Elevation of Privilege Vulnerability	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26617	In the Linux kernel, the following vulnerability has been resolved: fs/proc/task_mmu: move mmu notification mechanism inside mm lock Move mmu notification mechanism inside mm lock to prevent race condition in other components which depend on it. The notifier will invalidate memory range. Depending upon the number of iterations, different memory ranges would be invalidated. The following warning would be removed by this patch: WARNING: CPU: 0 PID: 5067 at arch/x86/kvm/../../../virt/kvm/kvm_main.c:734 kvm_mmu_notifier_change_pte+0x860/0x960 arch/x86/kvm/../../../virt/kvm/kvm_main.c:734 There is no behavioural and performance change with this patch when there is no component registered with the mmu notifier. [akpm@linux-foundation.org: narrow the scope of `range', per Sean]	7.0	More Details
CVE-2024-21439	Windows Telephony Server Elevation of Privilege Vulnerability	7.0	More Details
CVE-2024-27915	Sulu is a PHP content management system. Starting in verson 2.2.0 and prior to version 2.4.17 and 2.5.13, access to pages is granted regardless of role permissions for webspaces which have a security system configured and permission check enabled. Webspaces without do not have this issue. The problem is patched in versions 2.4.17 and 2.5.13. Some workarounds are available. One may apply the patch to `vendor/symfony/security-http/HttpUtils.php` manually or avoid installing `symfony/security-http` versions greater equal than `v5.4.30` or `v6.3.6`.	6.8	More Details
CVE-2024-21429	Windows USB Hub Driver Remote Code Execution Vulnerability	6.8	More Details
CVE-2024-28122	JWX is Go module implementing various JWx (JWA/JWE/JWK/JWS/JWT, otherwise known as JOSE) technologies. This vulnerability allows an attacker with a trusted public key to cause a Denial-of-Service (DoS) condition by crafting a malicious JSON Web Encryption (JWE) token with an exceptionally high compression ratio. This issue has been patched in versions 1.2.29 and 2.0.21.	6.8	More Details
CVE-2023-30968	One of Gotham Gaia services was found to be vulnerable to a stored cross-site scripting (XSS) vulnerability that could have allowed an attacker to bypass CSP and get a persistent cross site scripting payload on the stack.	6.8	More Details
CVE-2024-0044	In createSessionInternal of PackageInstallerService.java, there is a possible run-as any app due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	6.7	More Details
CVE-2024-25987	In pt_sysctl_command of pt.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	6.7	More Details
CVE-2024-23234	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to execute arbitrary code with kernel privileges.	6.7	More Details
CVE-2023-41842	A use of externally-controlled format string vulnerability [CWE-134] in Fortinet FortiManager version 7.4.0 through 7.4.1, version 7.2.0 through 7.2.3 and before 7.0.10, Fortinet FortiAnalyzer version 7.4.0 through 7.4.1, version 7.2.0 through 7.2.3 and before 7.0.10, Fortinet FortiAnalyzer-BigData before 7.2.5 and Fortinet FortiPortal version 6.0 all versions and version 5.3 all versions allows a privileged attacker to execute unauthorized code or commands via specially crafted command arguments.	6.7	More Details
CVE-2023-42509	JFrog Artifactory later than version 7.17.4 but prior to version 7.77.0 is vulnerable to an issue whereby a sequence of improperly handled exceptions in repository configuration initialization steps may lead to exposure of sensitive data.	6.6	More Details
CVE-2024-26201	Microsoft Intune Linux Agent Elevation of Privilege Vulnerability	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28753	RaspAP (aka raspap-webgui) through 3.0.9 allows remote attackers to read the /etc/passwd file via a crafted request.	6.5	More Details
CVE-2024-28120	codeium-chrome is an open source code completion plugin for the chrome web browser. The service worker of the codeium-chrome extension doesn't check the sender when receiving an external message. This allows an attacker to host a website that will steal the user's Codeium api-key, and thus impersonate the user on the backend autocomplete server. This issue has not been addressed. Users are advised to monitor the usage of their API key.	6.5	More Details
CVE-2024-27279	Directory traversal vulnerability exists in a-blog cms Ver.3.1.x series Ver.3.1.9 and earlier, Ver.3.0.x series Ver.3.0.30 and earlier, Ver.2.11.x series Ver.2.11.59 and earlier, Ver.2.10.x series Ver.2.10.51 and earlier, and Ver.2.9 and earlier versions. If this vulnerability is exploited, a user with editor or higher privilege who can login to the product may obtain arbitrary files on the server including password files.	6.5	More Details
CVE-2024-1227	An open redirect vulnerability, the exploitation of which could allow an attacker to create a custom URL and redirect a legitimate page to a malicious site.	6.5	More Details
CVE-2024-1303	Incorrectly limiting the path to a restricted directory vulnerability in Badger Meter Monitool that affects versions up to 4.6.3 and earlier. This vulnerability allows an authenticated attacker to retrieve any file from the device using the download-file functionality.	6.5	More Details
CVE-2024-1123	The EventPrime – Events Calendar, Bookings and Tickets plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the save_frontend_event_submission() function in all versions up to, and including, 3.4.2. This makes it possible for authenticated attackers, with subscriber-level access and above, to overwrite the title and content of arbitrary posts. This can also be exploited by unauthenticated attackers when the allow_submission_by_anonymous_user setting is enabled.	6.5	More Details
CVE-2023-43279	Null Pointer Dereference in mask_cidr6 component at cidr.c in Tcpreplay 4.4.4 allows attackers to crash the application via crafted tcprewrite command.	6.5	More Details
CVE-2024-2357	The Libreswan Project was notified of an issue causing libreswan to restart under some IKEv2 retransmit scenarios when a connection is configured to use PreSharedKeys (authby=secret) and the connection cannot find a matching configured secret. When such a connection is automatically added on startup using the auto= keyword, it can cause repeated crashes leading to a Denial of Service.	6.5	More Details
CVE-2024-0045	In smp_proc_sec_req of smp_act.cc, there is a possible out of bounds read due to improper input validation. This could lead to remote (proximal/adjacent) information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	6.5	More Details
CVE-2024-1125	The EventPrime – Events Calendar, Bookings and Tickets plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the calendar_events_delete() function in all versions up to, and including, 3.4.3. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary posts.	6.5	More Details
CVE-2024-2182	A flaw was found in the Open Virtual Network (OVN). In OVN clusters where BFD is used between hypervisors for high availability, an attacker can inject specially crafted BFD packets from inside unprivileged workloads, including virtual machines or containers, that can trigger a denial of service.	6.5	More Details
CVE-2024-1290	The User Registration WordPress plugin before 2.12 does not prevent users with at least the contributor role from rendering sensitive shortcodes, allowing them to generate, and leak, valid password reset URLs, which they can use to take over any accounts.	6.5	More Details
CVE-2024-26185	Windows Compressed Folder Tampering Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26197	Windows Standards-Based Storage Management Service Denial of Service Vulnerability	6.5	More Details
CVE-2024-2049	Server-Side Request Forgery (SSRF) in Citrix SD-WAN Standard/Premium Editions on or after 11.4.0 and before 11.4.4.46 allows an attacker to disclose limited information from the appliance via Access to management IP.	6.5	More Details
CVE-2024-1320	The EventPrime – Events Calendar, Bookings and Tickets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'offline_status' parameter in all versions up to, and including, 3.4.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.5	More Details
CVE-2024-23280	An injection issue was addressed with improved validation. This issue is fixed in Safari 17.4, macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4, watchOS 10.4, tvOS 17.4. A maliciously crafted webpage may be able to fingerprint the user.	6.5	More Details
CVE-2024-23259	The issue was addressed with improved checks. This issue is fixed in iOS 16.7.6 and iPadOS 16.7.6, iOS 17.4 and iPadOS 17.4, macOS Sonoma 14.4. Processing web content may lead to a denial-of-service.	6.5	More Details
CVE-2024-28111	Canarytokens helps track activity and actions on a network. Canarytokens.org supports exporting the history of a Canarytoken's incidents in CSV format. The generation of these CSV files is vulnerable to a CSV Injection vulnerability. This flaw can be used by an attacker who discovers an HTTP-based Canarytoken to target the Canarytoken's owner, if the owner exports the incident history to CSV and opens in a reader application such as Microsoft Excel. The impact is that this issue could lead to code execution on the machine on which the CSV file is opened. Version sha-c595a1f8 contains a fix for this issue.	6.5	More Details
CVE-2024-1299	A privilege escalation vulnerability was discovered in GitLab affecting versions 16.8 prior to 16.8.4 and 16.9 prior to 16.9.2. It was possible for a user with custom role of `manage_group_access_tokens` to rotate group access tokens with owner privileges.	6.5	More Details
CVE-2024-23284	A logic issue was addressed with improved state management. This issue is fixed in tvOS 17.4, macOS Sonoma 14.4, visionOS 1.1, iOS 17.4 and iPadOS 17.4, watchOS 10.4, iOS 16.7.6 and iPadOS 16.7.6, Safari 17.4. Processing maliciously crafted web content may prevent Content Security Policy from being enforced.	6.5	More Details
CVE-2024-23254	The issue was addressed with improved UI handling. This issue is fixed in tvOS 17.4, macOS Sonoma 14.4, visionOS 1.1, iOS 17.4 and iPadOS 17.4, watchOS 10.4, Safari 17.4. A malicious website may exfiltrate audio data cross-origin.	6.5	More Details
CVE-2024-20345	A vulnerability in the file upload functionality of Cisco AppDynamics Controller could allow an authenticated, remote attacker to conduct directory traversal attacks on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to an affected device. A successful exploit could allow the attacker to access sensitive data on an affected device.	6.5	More Details
CVE-2024-20336	A vulnerability in the web-based user interface of Cisco Small Business 100, 300, and 500 Series Wireless APs could allow an authenticated, remote attacker to perform buffer overflow attacks against an affected device. In order to exploit this vulnerability, the attacker must have valid administrative credentials for the device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20335	A vulnerability in the web-based management interface of Cisco Small Business 100, 300, and 500 Series Wireless APs could allow an authenticated, remote attacker to perform command injection attacks against an affected device. In order to exploit this vulnerability, the attacker must have valid administrative credentials for the device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system.	6.5	More Details
CVE-2024-23263	A logic issue was addressed with improved validation. This issue is fixed in tvOS 17.4, macOS Sonoma 14.4, visionOS 1.1, iOS 17.4 and iPadOS 17.4, watchOS 10.4, iOS 16.7.6 and iPadOS 16.7.6, Safari 17.4. Processing maliciously crafted web content may prevent Content Security Policy from being enforced.	6.5	More Details
CVE-2024-28149	Jenkins HTML Publisher Plugin 1.16 through 1.32 (both inclusive) does not properly sanitize input, allowing attackers with Item/Configure permission to implement cross-site scripting (XSS) attacks and to determine whether a path on the Jenkins controller file system exists.	6.5	More Details
CVE-2024-28229	In JetBrains YouTrack before 2024.1.25893 user without appropriate permissions could restore issues and articles	6.5	More Details
CVE-2024-28230	In JetBrains YouTrack before 2024.1.25893 attaching/detaching workflow to a project was possible without project admin permissions	6.5	More Details
CVE-2023-46170	IBM DS8900F HMC 89.21.19.0, 89.21.31.0, 89.30.68.0, 89.32.40.0, and 89.33.48.0 could allow an authenticated user to arbitrarily read files after enumerating file names.	6.5	More Details
CVE-2023-46169	IBM DS8900F HMC 89.21.19.0, 89.21.31.0, 89.30.68.0, 89.32.40.0, and 89.33.48.0 could allow an authenticated user to arbitrarily delete a file. IBM X-Force ID: 269406.	6.5	More Details
CVE-2024-27287	ESPHome is a system to control your ESP8266/ESP32 for Home Automation systems. Starting in version 2023.12.9 and prior to version 2024.2.2, editing the configuration file API in dashboard component of ESPHome version 2023.12.9 (command line installation and Home Assistant add-on) serves unsanitized data with `Content-Type: text/html; charset=UTF-8`, allowing a remote authenticated user to inject arbitrary web script and exfiltrate session cookies via Cross-Site scripting. It is possible for a malicious authenticated user to inject arbitrary Javascript in configuration files using a POST request to the /edit endpoint, the configuration parameter allows to specify the file to write. To trigger the XSS vulnerability, the victim must visit the page` /edit?configuration=[xss file]`. Abusing this vulnerability a malicious actor could perform operations on the dashboard on the behalf of a logged user, access sensitive information, create, edit and delete configuration files and flash firmware on managed boards. In addition to this, cookies are not correctly secured, allowing the exfiltration of session cookie values. Version 2024.2.2 contains a patch for this issue.	6.5	More Details
CVE-2024-28098	The vulnerability allows authenticated users with only produce or consume permissions to modify topic-level policies, such as retention, TTL, and offloading settings. These management operations should be restricted to users with the tenant admin role or super user role. This issue affects Apache Pulsar versions from 2.7.1 to 2.10.5, from 2.11.0 to 2.11.3, from 3.0.0 to 3.0.2, from 3.1.0 to 3.1.2, and 3.2.0. 2.10 Apache Pulsar users should upgrade to at least 2.10.6. 2.11 Apache Pulsar users should upgrade to at least 2.11.4. 3.0 Apache Pulsar users should upgrade to at least 3.0.3. 3.1 Apache Pulsar users should upgrade to at least 3.1.3. 3.2 Apache Pulsar users should upgrade to at least 3.2.1. Users operating versions prior to those listed above should upgrade to the aforementioned patched versions or newer versions.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1989	The Social Sharing Plugin – Sassy Social Share plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'Sassy_Social_Share' shortcode in all versions up to, and including, 3.3.58 due to insufficient input sanitization and output escaping on user supplied attributes such as 'url'. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1767	The Blocksy theme for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's blocks in all versions up to, and including, 2.0.26 due to insufficient input sanitization and output escaping on user supplied attributes like 'className' and 'radius'. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1421	The HT Mega – Absolute Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘border_type’ attribute of the Post Carousel widget in all versions up to, and including, 2.4.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2127	The Page Builder: Pagelayer – Drag and Drop website builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via custom attributes in all versions up to, and including, 1.8.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1366	The Happy Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘archive_title_tag’ attribute of the Archive Title widget in all versions up to, and including, 3.10.3 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-2024-1377	The Happy Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘author_meta_tag’ attribute of the Author Meta widget in all versions up to, and including, 3.10.3 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-2024-1419	The The Plus Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘_id’ attribute of the Header Meta Content widget in all versions up to, and including, 5.4.0 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-2024-1506	The Prime Slider – Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title_tags' attribute of the Fiestar widget in all versions up to, and including, 3.13.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-25990	In pktproc_perftest_gen_rx_packet_sktbuf_mode of link_rx_pktproc.c, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	6.4	More Details
CVE-2024-2136	The WPKoi Templates for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Advanced Heading widget 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 Number	Description	Base Score	Reference
CVE-2024-1534	The Booster for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 7.1.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1328	The Newsletter2Go plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘style’ parameter in all versions up to, and including, 4.0.13 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber 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-2024-1802	The EmbedPress – Embed PDF, Google Docs, Vimeo, Wistia, Embed YouTube Videos, Audios, Maps & Embed Any Documents in Gutenberg & Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Wistia embed block in all versions up to, and including, 3.9.10 due to insufficient input sanitization and output escaping on the user supplied url. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1761	The WP Chat App plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widget/block in all versions up to, and including, 3.6.1 due to insufficient input sanitization and output escaping on user supplied attributes such as 'buttonColor' and 'phoneNumber'. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2128	The EmbedPress – Embed PDF, Google Docs, Vimeo, Wistia, Embed YouTube Videos, Audios, Maps & Embed Any Documents in Gutenberg & Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's embed widget in all versions up to, and including, 3.9.10 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1987	The WP-Members Membership Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 3.4.9.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1397	The HT Mega – Absolute Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's blocks in all versions up to, and including, 2.4.6 due to insufficient input sanitization and output escaping on the 'titleTag' user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2031	The Video Conferencing with Zoom plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'zoom_recordings_by_meeting' shortcode in all versions up to, and including, 4.4.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2130	The CWW Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Module2 widget in all versions up to, and including, 1.2.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2352	A vulnerability, which was classified as critical, has been found in 1Panel up to 1.10.1-lts. Affected by this issue is the function baseApi.UpdateDeviceSwap of the file /api/v1/toolbox/device/update/swap. The manipulation of the argument Path with the input 123123123\nopen -a Calculator leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-256304.	6.3	More Details
CVE-2024-2332	A vulnerability was found in SourceCodester Online Mobile Management Store 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/maintenance/manage_category.php of the component HTTP GET Request Handler. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256283.	6.3	More Details
CVE-2024-2241	Improper access control in the user interface in Devolutions Workspace 2024.1.0 and earlier allows an authenticated user to perform unintended actions via specific permissions	6.3	More Details
CVE-2024-26492	An issue in Online Diagnostic Lab Management System 1.0 allows a remote attacker to gain control of a 'Staff' user account via a crafted POST request using the id, email, password, and cpass parameters.	6.3	More Details
CVE-2024-2281	A vulnerability was found in boyiddha Automated-Mess-Management-System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/index.php of the component Setting Handler. The manipulation leads to improper access controls. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256048. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-27297	Nix is a package manager for Linux and other Unix systems. A fixed-output derivations on Linux can send file descriptors to files in the Nix store to another program running on the host (or another fixed-output derivation) via Unix domain sockets in the abstract namespace. This allows to modify the output of the derivation, after Nix has registered the path as "valid" and immutable in the Nix database. In particular, this allows the output of fixed-output derivations to be modified from their expected content. This issue has been addressed in versions 2.3.18 2.18.2 2.19.4 and 2.20.5. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.3	More Details
CVE-2024-25103	This vulnerability exists in AppSamvid software due to the usage of vulnerable and outdated components. An attacker with local administrative privileges could exploit this by placing malicious DLLs on the targeted system. Successful exploitation of this vulnerability could allow the attacker to execute arbitrary code on the targeted system.	6.3	More Details
CVE-2024-1851	The affiliate-toolkit – WordPress Affiliate Plugin plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the atkp_create_list() function in all versions up to, and including, 3.5.4. This makes it possible for authenticated attackers, with subscriber-level access and above, to to perform unauthorized actions such as creating product lists.	6.3	More Details
CVE-2024-2351	A vulnerability classified as critical was found in CodeAstro Ecommerce Site 1.0. Affected by this vulnerability is an unknown functionality of the file action.php of the component Search. The manipulation of the argument cat_id/brand_id/keyword leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256303.	6.3	More Details
CVE-2024-24964	Improper access control vulnerability exists in the resident process of SKYSEA Client View versions from Ver.11.220 prior to Ver.19.2. If this vulnerability is exploited, an arbitrary process may be executed with SYSTEM privilege by a user who can log in to the PC where the product's Windows client is installed.	6.3	More Details
CVE-2024-2333	A vulnerability classified as critical has been found in CodeAstro Membership Management System 1.0. Affected is an unknown function of the file /add_members.php. The manipulation of the argument fullname leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256284.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2331	A vulnerability was found in SourceCodester Tourist Reservation System 1.0. It has been declared as critical. This vulnerability affects the function ad_writedata of the file System.cpp. The manipulation of the argument ad_code leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-256282 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-2269	A vulnerability was found in keerti1924 Online-Book-Store-Website 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /search.php. The manipulation of the argument search leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256039. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-1304	Cross-site scripting vulnerability in Badger Meter Monitool that affects versions up to 4.6.3 and earlier. This vulnerability allows a remote attacker to send a specially crafted javascript payload to an authenticated user and partially hijack their browser session.	6.3	More Details
CVE-2024-2330	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3. It has been classified as critical. This affects an unknown part of the file /protocol/index.php. The manipulation of the argument IPAddr leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256281 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-2329	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/list_resource_icon.php?action=delete. The manipulation of the argument IconId leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256280. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-28152	In Jenkins Bitbucket Branch Source Plugin 866.vdea_7dcd3008e and earlier, except 848.850.v6a_a_2a_234a_c81, when discovering pull requests from forks, the trust policy "Forks in the same account" allows changes to Jenkinsfiles from users without write access to the project when using Bitbucket Server.	6.3	More Details
CVE-2024-2283	A vulnerability classified as critical has been found in boyiddha Automated-Mess-Management-System 1.0. Affected is an unknown function of the file /member/view.php. The manipulation of the argument date leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-256050 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-2271	A vulnerability classified as critical has been found in keerti1924 Online-Book-Store-Website 1.0. This affects an unknown part of the file /shop.php of the component HTTP POST Request Handler. The manipulation of the argument product_name leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256041 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-2272	A vulnerability classified as critical was found in keerti1924 Online-Book-Store-Website 1.0. This vulnerability affects unknown code of the file /home.php of the component HTTP POST Request Handler. The manipulation of the argument product_name leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-256042 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-27288	1Panel is an open source Linux server operation and maintenance management panel. Prior to version 1.10.1-lts, users can use Burp to obtain unauthorized access to the console page. The vulnerability has been fixed in v1.10.1-lts. There are no known workarounds.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2393	A vulnerability was found in SourceCodester CRUD without Page Reload 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file add_user.php. The manipulation of the argument city leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256453 was assigned to this vulnerability.	6.3	More Details
CVE-2024-25984	In dumpBatteryDefend of dump_power.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	6.2	More Details
CVE-2024-20301	A vulnerability in Cisco Duo Authentication for Windows Logon and RDP could allow an authenticated, physical attacker to bypass secondary authentication and access an affected Windows device. This vulnerability is due to a failure to invalidate locally created trusted sessions after a reboot of the affected device. An attacker with primary user credentials could exploit this vulnerability by attempting to authenticate to an affected device. A successful exploit could allow the attacker to access the affected device without valid permissions.	6.2	More Details
CVE-2024-27612	Numbas editor before 7.3 mishandles editing of themes and extensions.	6.2	More Details
CVE-2024-24766	CasaOS-UserService provides user management functionalities to CasaOS. Starting in version 0.4.4.3 and prior to version 0.4.7, the Casa OS Login page disclosed the username enumeration vulnerability in the login page. An attacker can enumerate the CasaOS username using the application response. If the username is incorrect application gives the error `**User does not exist**`. If the password is incorrect application gives the error `**Invalid password**`. Version 0.4.7 fixes this issue.	6.2	More Details
CVE-2024-22007	In constraint_check of fvp.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	6.2	More Details
CVE-2022-43855	IBM SPSS Statistics 26.0, 27.0.1, and 28.0 could allow a local user to create multiple files that could exhaust the file handles capacity and cause a denial of service. IBM X-Force ID: 230235.	6.2	More Details
CVE-2024-2371	Information exposure vulnerability in Korenix JetI/O 6550 affecting firmware version F208 Build:0817. The SNMP protocol uses plaintext to transfer data, allowing an attacker to intercept traffic and retrieve credentials.	6.2	More Details
CVE-2023-49973	A cross-site scripting (XSS) vulnerability in Customer Support System v1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the email parameter at /customer_support/index.php?page=customer_list.	6.1	More Details
CVE-2023-49974	A cross-site scripting (XSS) vulnerability in Customer Support System v1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the contact parameter at /customer_support/index.php?page=customer_list.	6.1	More Details
CVE-2022-46089	Cross Site Scripting (XSS) vulnerability in the add-airline form of Online Flight Booking Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the airline parameter.	6.1	More Details
CVE-2024-1273	The Starbox WordPress plugin before 3.5.0 does not sanitise and escape some parameters, which could allow users with a role as low as Contributor to perform Cross-Site Scripting attacks	6.1	More Details
CVE-2024-2215	A cross-site request forgery (CSRF) vulnerability in Jenkins docker-build-step Plugin 2.11 and earlier allows attackers to connect to an attacker-specified TCP or Unix socket URL, and to reconfigure the plugin using the provided connection test parameters, affecting future build step executions.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43292	Cross Site Scripting vulnerability in My Food Recipe Using PHP with Source Code v.1.0 allows a local attacker to execute arbitrary code via a crafted payload to the Recipe Name, Procedure, and ingredients parameters.	6.1	More Details
CVE-2024-28823	Amazon AWS aws-js-s3-explorer (aka AWS JavaScript S3 Explorer) 1.0.0 allows XSS via a crafted S3 bucket name to index.html.	6.1	More Details
CVE-2023-42308	Cross Site Scripting (XSS) vulnerability in Manage Fastrack Subjects in Code-Projects Exam Form Submission 1.0 allows attackers to run arbitrary code via the "Subject Name" and "Subject Code" Section.	6.1	More Details
CVE-2024-24035	Cross Site Scripting (XSS) vulnerability in Setor Informatica SIL 3.1 allows attackers to run arbitrary code via the hmessage parameter.	6.1	More Details
CVE-2024-25327	Cross Site Scripting (XSS) vulnerability in Justice Systems FullCourt Enterprise v.8.2 allows a remote attacker to execute arbitrary code via the formatCaseNumber parameter of the Citation search function.	6.1	More Details
CVE-2023-49453	Reflected cross-site scripting (XSS) vulnerability in Racktables v0.22.0 and before, allows local attackers to execute arbitrary code and obtain sensitive information via the search component in index.php.	6.1	More Details
CVE-2024-25854	Cross Site Scripting (XSS) vulnerability in Sourcecodester Insurance Management System 1.0 allows attackers to run arbitrary code via the Subject and Description fields when submitting a support ticket.	6.1	More Details
CVE-2024-28112	Peering Manager is a BGP session management tool. Affected versions of Peering Manager are subject to a potential stored Cross-Site Scripting (XSS) attack in the `name` attribute of AS or Platform. The XSS triggers on a routers detail page. Adversaries are able to execute arbitrary JavaScript code with the permission of a victim. XSS attacks are often used to steal credentials or login tokens of other users. This issue has been addressed in version 1.8.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.1	More Details
CVE-2024-1442	A user with the permissions to create a data source can use Grafana API to create a data source with UID set to *. Doing this will grant the user access to read, query, edit and delete all data sources within the organization.	6.0	More Details
CVE-2024-25848	In the module "Ever Ultimate SEO" (everpsseo) <= 8.1.2 from Team Ever for PrestaShop, a guest can perform SQL injection in affected versions.	5.9	More Details
CVE-2024-27234	In fvp_set_target of fvp.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.9	More Details
CVE-2024-25989	In gpu_slc_liveness_update of pixel_gpu_slc.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.9	More Details
CVE-2024-1765	Cloudflare Quiche (through version 0.19.1/0.20.0) was affected by an unlimited resource allocation vulnerability causing rapid increase of memory usage of the system running quiche server or client. A remote attacker could take advantage of this vulnerability by repeatedly sending an unlimited number of 1-RTT CRYPTO frames after previously completing the QUIC handshake. Exploitation was possible for the duration of the connection which could be extended by the attacker. quiche 0.19.2 and 0.20.1 are the earliest versions containing the fix for this issue.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23277	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4. An attacker in a privileged network position may be able to inject keystrokes by spoofing a keyboard.	5.9	More Details
CVE-2024-26000	An unauthenticated remote attacker can read memory out of bounds due to improper input validation in the MQTT stack. The brute force attack is not always successful because of memory randomization.	5.9	More Details
CVE-2023-34980	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 4.5.4.2627 build 20231225 and later QuTS hero h4.5.4.2626 build 20231225 and later	5.9	More Details
CVE-2024-2236	A timing-based side-channel flaw was found in libgcrypt's RSA implementation. This issue may allow a remote attacker to initiate a Bleichenbacher-style attack, which can lead to the decryption of RSA ciphertexts.	5.9	More Details
CVE-2024-2107	The Blossom Spa theme for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.3.4 via generated source. This makes it possible for unauthenticated attackers to extract sensitive data including contents of password-protected or scheduled posts.	5.8	More Details
CVE-2024-28174	In JetBrains TeamCity before 2023.11.4 presigned URL generation requests in S3 Artifact Storage plugin were authorized improperly	5.8	More Details
CVE-2023-32264	CWE-1385 vulnerability in OpenText Documentum D2 affecting versions16.5.1 to CE 23.2. The vulnerability could allow upload arbitrary code and execute it on the client's computer.	5.8	More Details
CVE-2024-21430	Windows USB Attached SCSI (UAS) Protocol Remote Code Execution Vulnerability	5.7	More Details
CVE-2024-1460	MSI Afterburner v4.6.5.16370 is vulnerable to a Kernel Memory Leak vulnerability by triggering the 0x80002040 IOCTL code of the RTCore64.sys driver. The handle to the driver can only be obtained from a high integrity process.	5.6	More Details
CVE-2023-46172	IBM DS8900F HMC 89.21.19.0, 89.21.31.0, 89.30.68.0, 89.32.40.0, and 89.33.48.0 could allow a remote attacker to bypass authentication restrictions for authorized user. IBM X-Force ID: 269409.	5.6	More Details
CVE-2023-6814	Insertion of Sensitive Information into Log File vulnerability in Hitachi Cosminexus Component Container allows local users to gain sensitive information.This issue affects Cosminexus Component Container: from 11-30 before 11-30-05, from 11-20 before 11-20-07, from 11-10 before 11-10-10, from 11-00 before 11-00-12, All versions of V8 and V9.	5.6	More Details
CVE-2023-52498	In the Linux kernel, the following vulnerability has been resolved: PM: sleep: Fix possible deadlocks in core system-wide PM code It is reported that in low-memory situations the system-wide resume core code deadlocks, because async_schedule_dev() executes its argument function synchronously if it cannot allocate memory (and not only in that case) and that function attempts to acquire a mutex that is already held. Executing the argument function synchronously from within dpm_async_fn() may also be problematic for ordering reasons (it may cause a consumer device's resume callback to be invoked before a requisite supplier device's one, for example). Address this by changing the code in question to use async_schedule_dev_nocall() for scheduling the asynchronous execution of device suspend and resume functions and to directly run them synchronously if async_schedule_dev_nocall() returns false.	5.5	More Details
CVE-2024-23230	This issue was addressed with improved file handling. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to access sensitive user data.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52493	In the Linux kernel, the following vulnerability has been resolved: bus: mhi: host: Drop chan lock before queuing buffers Ensure read and write locks for the channel are not taken in succession by dropping the read lock from parse_xfer_event() such that a callback given to client can potentially queue buffers and acquire the write lock in that process. Any queueing of buffers should be done without channel read lock acquired as it can result in multiple locks and a soft lockup. [mani: added fixes tag and cc'ed stable]	5.5	More Details
CVE-2024-23264	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Monterey 12.7.4, macOS Ventura 13.6.5, macOS Sonoma 14.4, visionOS 1.1, iOS 17.4 and iPadOS 17.4, iOS 16.7.6 and iPadOS 16.7.6, tvOS 17.4. An application may be able to read restricted memory.	5.5	More Details
CVE-2024-23266	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2023-41015	code-projects.org Online Job Portal 1.0 is vulnerable to SQL Injection via /Employer/DeleteJob.php?JobId=1.	5.5	More Details
CVE-2024-23201	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Monterey 12.7.4, watchOS 10.3, tvOS 17.3, macOS Ventura 13.6.5, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3. An app may be able to cause a denial-of-service.	5.5	More Details
CVE-2023-28826	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 16.7.6 and iPadOS 16.7.6, macOS Monterey 12.7.4, macOS Sonoma 14.1, macOS Ventura 13.6.5. An app may be able to access sensitive user data.	5.5	More Details
CVE-2023-45793	A vulnerability has been identified in Siveillance Control (All versions >= V2.8 < V3.1.1). The affected product does not properly check the list of access groups that are assigned to an individual user. This could enable a locally logged on user to gain write privileges for objects where they only have read privileges.	5.5	More Details
CVE-2024-23267	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to bypass certain Privacy preferences.	5.5	More Details
CVE-2024-23269	A downgrade issue affecting Intel-based Mac computers was addressed with additional code-signing restrictions. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2024-23272	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. A user may gain access to protected parts of the file system.	5.5	More Details
CVE-2024-1441	An off-by-one error flaw was found in the udevListInterfacesByStatus() function in libvirt when the number of interfaces exceeds the size of the `names` array. This issue can be reproduced by sending specially crafted data to the libvirt daemon, allowing an unprivileged client to perform a denial of service attack by causing the libvirt daemon to crash.	5.5	More Details
CVE-2024-26627	In the Linux kernel, the following vulnerability has been resolved: scsi: core: Move scsi_host_busy() out of host lock for waking up EH handler Inside scsi_eh_wakeup(), scsi_host_busy() is called & checked with host lock every time for deciding if error handler kthread needs to be waken up. This can be too heavy in case of recovery, such as: - N hardware queues - queue depth is M for each hardware queue - each scsi_host_busy() iterates over (N * M) tag/requests If recovery is triggered in case that all requests are in-flight, each scsi_eh_wakeup() is strictly serialized, when scsi_eh_wakeup() is called for the last in-flight request, scsi_host_busy() has been run for (N * M - 1) times, and request has been iterated for (N*M - 1) * (N * M) times. If both N and M are big enough, hard lockup can be triggered on acquiring host lock, and it is observed on mpi3mr(128 hw queues, queue depth 8169). Fix the issue by calling scsi_host_busy() outside the host lock. We don't need the host lock for getting busy count because host the lock never covers that. [mkp: Drop unnecessary 'busy' variables pointed out by Bart]	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26626	In the Linux kernel, the following vulnerability has been resolved: ipmr: fix kernel panic when forwarding mcast packets The stacktrace was: [86.305548] BUG: kernel NULL pointer dereference, address: 0000000000000092 [86.306815] #PF: supervisor read access in kernel mode [86.307717] #PF: error_code(0x0000) - not-present page [86.308624] PGD 0 P4D 0 [86.309091] Oops: 0000 [#1] PREEMPT SMP NOPTI [86.309883] CPU: 2 PID: 3139 Comm: pimd Tainted: G U 6.8.0-6wind-knet #1 [86.311027] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.11.1-0-g0551a4be2c-prebuilt.qemu-project.org 04/01/2014 [86.312728] RIP: 0010:ip_mr_forward (/build/work/knet/net/ipv4/ipmr.c:1985) [86.313399] Code: f9 1f 0f 87 85 03 00 00 48 8d 04 5b 48 8d 04 83 49 8d 44 c5 00 48 8b 40 70 48 39 c2 0f 84 d9 00 00 00 49 8b 46 58 48 83 e0 fe <80> b8 92 00 00 00 00 0f 84 55 ff ff ff 49 83 47 38 01 45 85 e4 0f [86.316565] RSP: 0018:ffffad21c0583ae0 EFLAGS: 00010246 [86.317497] RAX: 0000000000000000 RBX: 0000000000000000 RCX: 0000000000000000 [86.318596] RDX: ffff9559cb46c000 RSI: 0000000000000000 RDI: 0000000000000000 [86.319627] RBP: ffffad21c0583b30 R08: 0000000000000000 R09: 0000000000000000 [86.320650] R10: 0000000000000000 R11: 0000000000000000 R12: 0000000000000001 [86.321672] R13: ffff9559c093a000 R14: ffff9559cc00b800 R15: ffff9559c09c1d80 [86.322873] FS: 00007f85db661980(0000) GS:ffff955a79d00000(0000) knlGS:0000000000000000 [86.324291] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [86.325314] CR2: 0000000000000092 CR3: 000000002f13a000 CR4: 0000000000350ef0 [86.326589] Call Trace: [86.327036] <TASK> [86.327434] ? show_regs (/build/work/knet/arch/x86/kernel/dumpstack.c:479) [86.328049] ? __die (/build/work/knet/arch/x86/kernel/dumpstack.c:421 /build/work/knet/arch/x86/kernel/dumpstack.c:434) [86.328508] ? page_fault_oops (/build/work/knet/arch/x86/mm/fault.c:707) [86.329107] ? do_user_addr_fault (/build/work/knet/arch/x86/mm/fault.c:1264) [86.329756] ? srso_return_thunk (/build/work/knet/arch/x86/lib/retpoline.S:223) [86.330350] ? __irq_work_queue_local (/build/work/knet/kernel/irq_work.c:111 (discriminator 1)) [86.331013] ? exc_page_fault (/build/work/knet/./arch/x86/include/asm/paravirt.h:693 /build/work/knet/arch/x86/mm/fault.c:1515 /build/work/knet/arch/x86/mm/fault.c:1563) [86.331702] ? asm_exc_page_fault (/build/work/knet/./arch/x86/include/asm/idtentry.h:570) [86.332468] ? ip_mr_forward (/build/work/knet/net/ipv4/ipmr.c:1985) [86.333183] ? srso_return_thunk (/build/work/knet/arch/x86/lib/retpoline.S:223) [86.333920] ipmr_mfc_add (/build/work/knet/./include/linux/rcupdate.h:782 /build/work/knet/net/ipv4/ipmr.c:1009 /build/work/knet/net/ipv4/ipmr.c:1273) [86.334583] ? __pfx_ipmr_hash_cmp (/build/work/knet/net/ipv4/ipmr.c:363) [86.335357] ip_mroute_setsockopt (/build/work/knet/net/ipv4/ipmr.c:1470) [86.336135] ? srso_return_thunk (/build/work/knet/arch/x86/lib/retpoline.S:223) [86.336854] ? ip_mroute_setsockopt (/build/work/knet/net/ipv4/ipmr.c:1470) [86.337679] do_ip_setsockopt (/build/work/knet/net/ipv4/ip_sockglue.c:944) [86.338408] ? __pfx_unix_stream_read_actor (/build/work/knet/net/unix/af_unix.c:2862) [86.339232] ? srso_return_thunk (/build/work/knet/arch/x86/lib/retpoline.S:223) [86.339809] ? aa_sk_perm (/build/work/knet/security/apparmor/include/cred.h:153 /build/work/knet/security/apparmor/net.c:181) [86.340342] ip_setsockopt (/build/work/knet/net/ipv4/ip_sockglue.c:1415) [86.340859] raw_setsockopt (/build/work/knet/net/ipv4/raw.c:836) [86.341408] ? security_socket_setsockopt (/build/work/knet/security/security.c:4561 (discriminator 13)) [86.342116] sock_common_setsockopt (/build/work/knet/net/core/sock.c:3716) [86.342747] do_sock_setsockopt (/build/work/knet/net/socket.c:2313) [86.343363] __sys_setsockopt (/build/work/knet/./include/linux/file.h:32 /build/work/kn ---truncated---	5.5	More Details
CVE-2024-26174	Windows Kernel Information Disclosure Vulnerability	5.5	More Details
CVE-2024-26177	Windows Kernel Information Disclosure Vulnerability	5.5	More Details
CVE-2024-22889	Due to incorrect access control in Plone version v6.0.9, remote attackers can view and list all files hosted on the website via sending a crafted request.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26181	Windows Kernel Denial of Service Vulnerability	5.5	More Details
CVE-2023-52607	In the Linux kernel, the following vulnerability has been resolved: powerpc/mm: Fix null-pointer dereference in pgtable_cache_add kasprintf() returns a pointer to dynamically allocated memory which can be NULL upon failure. Ensure the allocation was successful by checking the pointer validity.	5.5	More Details
CVE-2023-52595	In the Linux kernel, the following vulnerability has been resolved: wifi: rt2x00: restart beacon queue when hardware reset When a hardware reset is triggered, all registers are reset, so all queues are forced to stop in hardware interface. However, mac80211 will not automatically stop the queue. If we don't manually stop the beacon queue, the queue will be deadlocked and unable to start again. This patch fixes the issue where Apple devices cannot connect to the AP after calling ieee80211_restart_hw().	5.5	More Details
CVE-2023-52593	In the Linux kernel, the following vulnerability has been resolved: wifi: wfx: fix possible NULL pointer dereference in wfx_set_mfp_ap() Since 'ieee80211_beacon_get()' can return NULL, 'wfx_set_mfp_ap()' should check the return value before examining skb data. So convert the latter to return an appropriate error code and propagate it to return from 'wfx_start_ap()' as well. Compile tested only.	5.5	More Details
CVE-2023-52585	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix possible NULL dereference in amdgpu_ras_query_error_status_helper() Return invalid error code -EINVAL for invalid block id. Fixes the below: drivers/gpu/drm/amd/amdgpu/amdgpu_ras.c:1183 amdgpu_ras_query_error_status_helper() error: we previously assumed 'info' could be null (see line 1176)	5.5	More Details
CVE-2024-23279	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.4. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2024-27235	In plugin_extern_func of , there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-23281	This issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.4. An app may be able to access sensitive user data.	5.5	More Details
CVE-2024-23283	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 16.7.6 and iPadOS 16.7.6, macOS Monterey 12.7.4, macOS Sonoma 14.4, macOS Ventura 13.6.5. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2024-23290	A logic issue was addressed with improved restrictions. This issue is fixed in tvOS 17.4, iOS 17.4 and iPadOS 17.4, macOS Sonoma 14.4, watchOS 10.4. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2024-23285	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Sonoma 14.4. An app may be able to create symlinks to protected regions of the disk.	5.5	More Details
CVE-2024-23220	The issue was addressed with improved handling of caches. This issue is fixed in visionOS 1.1, iOS 17.4 and iPadOS 17.4. An app may be able to fingerprint the user.	5.5	More Details
CVE-2024-23205	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4. An app may be able to access sensitive user data.	5.5	More Details
CVE-2024-26160	Windows Cloud Files Mini Filter Driver Information Disclosure Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26615	In the Linux kernel, the following vulnerability has been resolved: net/smc: fix illegal rmb_desc access in SMC-D connection dump A crash was found when dumping SMC-D connections. It can be reproduced by following steps: - run nginx/wrk test: smc_run nginx smc_run wrk -t 16 -c 1000 -d <duration> -H 'Connection: Close' <URL> - continuously dump SMC-D connections in parallel: watch -n 1 'smcss -D' BUG: kernel NULL pointer dereference, address: 0000000000000030 CPU: 2 PID: 7204 Comm: smcss Kdump: loaded Tainted: G E 6.7.0+ #55 RIP: 0010:__smc_diag_dump.constprop.0+0x5e5/0x620 [smc_diag] Call Trace: <TASK> ? __die+0x24/0x70 ? page_fault_oops+0x66/0x150 ? exc_page_fault+0x69/0x140 ? asm_exc_page_fault+0x26/0x30 ? __smc_diag_dump.constprop.0+0x5e5/0x620 [smc_diag] ? __kmalloc_node_track_caller+0x35d/0x430 ? __alloc_skb+0x77/0x170 smc_diag_dump_proto+0xd0/0xf0 [smc_diag] smc_diag_dump+0x26/0x60 [smc_diag] netlink_dump+0x19f/0x320 __netlink_dump_start+0x1dc/0x300 smc_diag_handler_dump+0x6a/0x80 [smc_diag] ? __pfx_smc_diag_dump+0x10/0x10 [smc_diag] sock_diag_rcv_msg+0x121/0x140 ? __pfx_sock_diag_rcv_msg+0x10/0x10 netlink_rcv_skb+0x5a/0x110 sock_diag_rcv+0x28/0x40 netlink_unicast+0x22a/0x330 netlink_sendmsg+0x1f8/0x420 __sock_sendmsg+0xb0/0xc0 ____sys_sendmsg+0x24e/0x300 ? copy_msghdr_from_user+0x62/0x80 ___sys_sendmsg+0x7c/0xd0 ? __do_fault+0x34/0x160 ? do_read_fault+0x5f/0x100 ? do_fault+0xb0/0x110 ? __handle_mm_fault+0x2b0/0x6c0 __sys_sendmsg+0x4d/0x80 do_syscall_64+0x69/0x180 entry_SYSCALL_64_after_hwframe+0x6e/0x76 It is possible that the connection is in process of being established when we dump it. Assumed that the connection has been registered in a link group by smc_conn_create() but the rmb_desc has not yet been initialized by smc_buf_create(), thus causing the illegal access to conn->rmb_desc. So fix it by checking before dump.	5.5	More Details
CVE-2024-23250	An access issue was addressed with improved access restrictions. This issue is fixed in tvOS 17.4, iOS 17.4 and iPadOS 17.4, macOS Sonoma 14.4, watchOS 10.4. An app may be able to access Bluetooth-connected microphones without user permission.	5.5	More Details
CVE-2023-47221	A path traversal vulnerability has been reported to affect Photo Station. If exploited, the vulnerability could allow authenticated administrators to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following version: Photo Station 6.4.2 (2023/12/15) and later	5.5	More Details
CVE-2024-21408	Windows Hyper-V Denial of Service Vulnerability	5.5	More Details
CVE-2024-23287	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4, watchOS 10.4. An app may be able to access user-sensitive data.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52487	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Fix peer flow lists handling The cited change refactored mlx5e_tc_del_fdb_peer_flow() to only clear DUP flag when list of peer flows has become empty. However, if any concurrent user holds a reference to a peer flow (for example, the neighbor update workqueue task is updating peer flow's parent encap entry concurrently), then the flow will not be removed from the peer list and, consecutively, DUP flag will remain set. Since mlx5e_tc_del_fdb_peers_flow() calls mlx5e_tc_del_fdb_peer_flow() for every possible peer index the algorithm will try to remove the flow from eswitch instances that it has never peered with causing either NULL pointer dereference when trying to remove the flow peer list head of peer_index that was never initialized or a warning if the list debug config is enabled[0]. Fix the issue by always removing the peer flow from the list even when not releasing the last reference to it. [0]: [3102.985806] ------------[cut here]------------ [3102.986223] list_del corruption, ffff888139110698->next is NULL [3102.986757] WARNING: CPU: 2 PID: 22109 at lib/list_debug.c:53 __list_del_entry_valid_or_report+0x4f/0xc0 [3102.987561] Modules linked in: act_ct nf_flow_table bonding act_tunnel_key act_mirred act_skbedit vxlan cls_matchall nfnetlink_cttimeout act_gact cls_flower sch_ingress mlx5_vdpa vringh vhost_iotlb vdpa openvswitch nsh xt_MASQUERADE nf_conntrack_netlink nfnetlink iptable_nat xt_addrtype xt_conntrack nf_nat br_netfilter rpcsec_gss_krb5 auth_rpcg ss oid_registry overlay rpcrdma rdma_ucm ib_iser libiscsi scsi_transport_iscsi ib_umad rdma_cm ib_ipoib iw_cm ib_cm mlx5_ib ib_uverbs ib_core mlx5_core [last unloaded: bonding] [3102.991113] CPU: 2 PID: 22109 Comm: revalidator28 Not tainted 6.6.0-rc6+ #3 [3102.991695] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.13.0-0-gf21b5a4aeb02-prebuilt.qemu.org 04/01/2014 [3102.992605] RIP: 0010:__list_del_entry_valid_or_report+0x4f/0xc0 [3102.993122] Code: 39 c2 74 56 48 8b 32 48 39 fe 75 62 48 8b 51 08 48 39 f2 75 73 b8 01 00 00 00 c3 48 89 fe 48 c7 c7 48 fd 0a 82 e8 41 0b ad ff <0f> 0b 31 c0 c3 48 89 fe 48 c7 c7 70 fd 0a 82 e8 2d 0b ad ff 0f 0b [3102.994615] RSP: 0018:ffff8881383e7710 EFLAGS: 00010286 [3102.995078] RAX: 0000000000000000 RBX: 0000000000000002 RCX: 0000000000000000 [3102.995670] RDX: 0000000000000001 RSI: ffff88885f89b640 RDI: ffff88885f89b640 [3102.997188] DEL flow 00000000be367878 on port 0 [3102.998594] RBP: dead000000000122 R08: 0000000000000000 R09: c0000000ffffdfff [3102.999604] R10: 0000000000000008 R11: ffff8881383e7598 R12: dead000000000100 [3103.000198] R13: 0000000000000002 R14: ffff888139110000 R15: ffff888101901240 [3103.000790] FS: 00007f424cde4700(0000) GS:ffff88885f880000(0000) knlGS:0000000000000000 [3103.001486] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [3103.001986] CR2: 00007fd42e8dcb70 CR3: 000000011e68a003 CR4: 0000000000370ea0 [3103.002596] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [3103.003190] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [3103.003787] Call Trace: [3103.004055] <TASK> [3103.004297] ? __warn+0x7d/0x130 [3103.004623] ? __list_del_entry_valid_or_report+0x4f/0xc0 [3103.005094] ? report_bug+0xf1/0x1c0 [3103.005439] ? console_unlock+0x4a/0xd0 [3103.005806] ? handle_bug+0x3f/0x70 [3103.006149] ? exc_invalid_op+0x13/0x60 [3103.006531] ? asm_exc_invalid_op+0x16/0x20 [3103.007430] ? __list_del_entry_valid_or_report+0x4f/0xc0 [3103.007910] mlx5e_tc_del_fdb_peers_flow+0xcf/0x240 [mlx5_core] [3103.008463] mlx5e_tc_del_flow+0x46/0x270 [mlx5_core] [3103.008944] mlx5e_flow_put+0x26/0x50 [mlx5_core] [3103.009401] mlx5e_delete_flower+0x25f/0x380 [mlx5_core] [3103.009901] tc_setup_cb_destroy+0xab/0x180 [3103.010292] fl_hw_destroy_filter+0x99/0xc0 [cls_flower] [3103.010779] __fl_delete+0x2d4/0x2f0 [cls_flower] [3103.0 ---truncated---	5.5	More Details
CVE-2024-23241	This issue was addressed through improved state management. This issue is fixed in tvOS 17.4, iOS 17.4 and iPadOS 17.4, macOS Sonoma 14.4. An app may be able to leak sensitive user information.	5.5	More Details
CVE-2024-26612	In the Linux kernel, the following vulnerability has been resolved: netfs, fscache: Prevent Oops in fscache_put_cache() This function dereferences "cache" and then checks if it's IS_ERR_OR_NULL(). Check first, then dereference.	5.5	More Details
CVE-2024-20671	Microsoft Defender Security Feature Bypass Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26614	In the Linux kernel, the following vulnerability has been resolved: tcp: make sure init the accept_queue's spinlocks once When I run syz's reproduction C program locally, it causes the following issue: pvqspinlock: lock 0xffff9d181cd5c660 has corrupted value 0x0! WARNING: CPU: 19 PID: 21160 at __pv_queued_spin_unlock_slowpath (kernel/locking/qspinlock_paravirt.h:508) Hardware name: Red Hat KVM, BIOS 0.5.1 01/01/2011 RIP: 0010:__pv_queued_spin_unlock_slowpath (kernel/locking/qspinlock_paravirt.h:508) Code: 73 56 3a ff 90 c3 cc cc cc cc 8b 05 bb 1f 48 01 85 c0 74 05 c3 cc cc cc cc 8b 17 48 89 fe 48 c7 c7 30 20 ce 8f e8 ad 56 42 ff <0f> 0b c3 cc cc cc cc 0f 0b 0f 1f 40 00 90 90 90 90 90 90 90 90 90 RSP: 0018:ffffa8d200604cb8 EFLAGS: 00010282 RAX: 0000000000000000 RBX: 0000000000000000 RCX: ffff9d1ef60e0908 RDX: 00000000ffffffd8 RSI: 0000000000000027 RDI: ffff9d1ef60e0900 RBP: ffff9d181cd5c280 R08: 0000000000000000 R09: 00000000ffff7fff R10: ffffa8d200604b68 R11: ffffffff907dcdc8 R12: 0000000000000000 R13: ffff9d181cd5c660 R14: ffff9d1813a3f330 R15: 0000000000001000 FS: 00007fa110184640(0000) GS:ffff9d1ef60c0000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000020000000 CR3: 000000011f65e000 CR4: 00000000000006f0 Call Trace: <IRQ> _raw_spin_unlock (kernel/locking/spinlock.c:186) inet_csk_reqsk_queue_add (net/ipv4/inet_connection_sock.c:1321) inet_csk_complete_hashdance (net/ipv4/inet_connection_sock.c:1358) tcp_check_req (net/ipv4/tcp_minisocks.c:868) tcp_v4_rcv (net/ipv4/tcp_ipv4.c:2260) ip_protocol_deliver_rcu (net/ipv4/ip_input.c:205) ip_local_deliver_finish (net/ipv4/ip_input.c:234) __netif_receive_skb_one_core (net/core/dev.c:5529) process_backlog (./include/linux/rcupdate.h:779) __napi_poll (net/core/dev.c:6533) net_rx_action (net/core/dev.c:6604) __do_softirq (./arch/x86/include/asm/jump_label.h:27) do_softirq (kernel/softirq.c:454 kernel/softirq.c:441) </IRQ> <TASK> __local_bh_enable_ip (kernel/softirq.c:381) __dev_queue_xmit (net/core/dev.c:4374) ip_finish_output2 (./include/net/neighbour.h:540 net/ipv4/ip_output.c:235) __ip_queue_xmit (net/ipv4/ip_output.c:535) __tcp_transmit_skb (net/ipv4/tcp_output.c:1462) tcp_rcv_synsent_state_process (net/ipv4/tcp_input.c:6469) tcp_rcv_state_process (net/ipv4/tcp_input.c:6657) tcp_v4_do_rcv (net/ipv4/tcp_ipv4.c:1929) __release_sock (./include/net/sock.h:1121 net/core/sock.c:2968) release_sock (net/core/sock.c:3536) inet_wait_for_connect (net/ipv4/af_inet.c:609) __inet_stream_connect (net/ipv4/af_inet.c:702) inet_stream_connect (net/ipv4/af_inet.c:748) __sys_connect (./include/linux/file.h:45 net/socket.c:2064) __x64_sys_connect (net/socket.c:2073 net/socket.c:2070 net/socket.c:2070) do_syscall_64 (arch/x86/entry/common.c:51 arch/x86/entry/common.c:82) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:129) RIP: 0033:0x7fa10ff05a3d Code: 5b 41 5c c3 66 0f 1f 84 00 00 00 00 00 f3 0f 1e fa 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 8b 0d ab a3 0e 00 f7 d8 64 89 01 48 RSP: 002b:00007fa110183de8 EFLAGS: 00000202 ORIG_RAX: 000000000000002a RAX: ffffffffffffffda RBX: 0000000020000054 RCX: 00007fa10ff05a3d RDX: 000000000000001c RSI: 0000000020000040 RDI: 0000000000000003 RBP: 00007fa110183e20 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000202 R12: 00007fa110184640 R13: 0000000000000000 R14: 00007fa10fe8b060 R15: 00007fff73e23b20 </TASK> The issue triggering process is analyzed as follows: Thread A Thread B tcp_v4_rcv //receive ack TCP packet inet_shutdown tcp_check_req tcp_disconnect //disconnect sock ... tcp_set_state(sk, TCP_CLOSE) inet_csk_complete_hashdance ... inet_csk_reqsk_queue_add ---truncated---	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26611	In the Linux kernel, the following vulnerability has been resolved: xsk: fix usage of multi-buffer BPF helpers for ZC XDP Currently when packet is shrunk via bpf_xdp_adjust_tail() and memory type is set to MEM_TYPE_XSK_BUFF_POOL, null ptr dereference happens: [1136314.192256] BUG: kernel NULL pointer dereference, address: 0000000000000034 [1136314.203943] #PF: supervisor read access in kernel mode [1136314.213768] #PF: error_code(0x0000) - not-present page [1136314.223550] PGD 0 P4D 0 [1136314.230684] Oops: 0000 [#1] PREEMPT SMP NOPTI [1136314.239621] CPU: 8 PID: 54203 Comm: xdpsock Not tainted 6.6.0+ #257 [1136314.250469] Hardware name: Intel Corporation S2600WFT/S2600WFT, BIOS SE5C620.86B.02.01.0008.031920191559 03/19/2019 [1136314.265615] RIP: 0010:__xdp_return+0x6c/0x210 [1136314.274653] Code: ad 00 48 8b 47 08 49 89 f8 a8 01 0f 85 9b 01 00 00 0f 1f 44 00 00 f0 41 ff 48 34 75 32 4c 89 c7 e9 79 cd 80 ff 83 fe 03 75 17 <f6> 41 34 01 0f 85 02 01 00 00 48 89 cf e9 22 cc 1e 00 e9 3d d2 86 [1136314.302907] RSP: 0018:ffffc900089f8db0 EFLAGS: 00010246 [1136314.312967] RAX: ffffc9003168aed0 RBX: ffff8881c3300000 RCX: 0000000000000000 [1136314.324953] RDX: 0000000000000000 RSI: 0000000000000003 RDI: ffffc9003168c000 [1136314.336929] RBP: 0000000000000ae0 R08: 0000000000000002 R09: 0000000000010000 [1136314.348844] R10: ffffc9000e495000 R11: 0000000000000040 R12: 0000000000000001 [1136314.360706] R13: 0000000000000524 R14: ffffc9003168aec0 R15: 0000000000000001 [1136314.373298] FS: 00007f8df8bbcb80(0000) GS:ffff8897e0e00000(0000) knlGS:0000000000000000 [1136314.386105] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [1136314.396532] CR2: 0000000000000034 CR3: 00000001aa912002 CR4: 0000000007706f0 [1136314.408377] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [1136314.420173] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [1136314.431890] PKRU: 55555554 [1136314.439143] Call Trace: [1136314.446058] <IRQ> [1136314.452465] ? __die+0x20/0x70 [1136314.459881] ? page_fault_oops+0x15b/0x440 [1136314.468305] ? exc_page_fault+0x6a/0x150 [1136314.476491] ? asm_exc_page_fault+0x22/0x30 [1136314.484927] ? __xdp_return+0x6c/0x210 [1136314.492863] bpf_xdp_adjust_tail+0x155/0x1d0 [1136314.501269] bpf_prog_ccc47ae29d3b6570_xdp_sock_prog+0x15/0x60 [1136314.511263] ice_clean_rx_irq_zc+0x206/0xc60 [ice] [1136314.520222] ? ice_xmit_zc+0x6e/0x150 [ice] [1136314.528506] ice_napi_poll+0x467/0x670 [ice] [1136314.536858] ? ttwu_do_activate.constprop.0+0x8f/0x1a0 [1136314.546010] __napi_poll+0x29/0x1b0 [1136314.553462] net_rx_action+0x133/0x270 [1136314.561619] __do_softirq+0xbe/0x28e [1136314.569303] do_softirq+0x3f/0x60 This comes from __xdp_return() call with xdp_buff argument passed as NULL which is supposed to be consumed by xsk_buff_free() call. To address this properly, in ZC case, a node that represents the frag being removed has to be pulled out of xskb_list. Introduce appropriate xsk helpers to do such node operation and use them accordingly within bpf_xdp_adjust_tail().	5.5	More Details
CVE-2024-23297	The issue was addressed with improved checks. This issue is fixed in tvOS 17.4, iOS 17.4 and iPadOS 17.4, watchOS 10.4. A malicious application may be able to access private information.	5.5	More Details
CVE-2024-23295	A permissions issue was addressed to help ensure Personas are always protected This issue is fixed in visionOS 1.1. An unauthenticated user may be able to use an unprotected Persona.	5.5	More Details
CVE-2024-0047	In writeUserLP of UserManagerService.java, device policies are serialized with an incorrect tag due to a logic error in the code. This could lead to local denial of service when policies are deserialized on reboot with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-22010	In dvfs_plugin_caller of fvp.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-23260	This issue was addressed by removing additional entitlements. This issue is fixed in macOS Sonoma 14.4. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2024-23231	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.6.5, macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4, watchOS 10.4, iOS 16.7.6 and iPadOS 16.7.6. An app may be able to access user-sensitive data.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20346	A vulnerability in the web-based management interface of Cisco AppDynamics Controller could allow an authenticated, remote attacker to perform a reflected cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	5.4	More Details
CVE-2024-28339	An information leak in the debuginfo.htm component of Netgear CBR40 2.5.0.28, Netgear CBK40 2.5.0.28, and Netgear CBK43 2.5.0.28 allows attackers to obtain sensitive information without any authentication required.	5.4	More Details
CVE-2024-24097	Cross Site Scripting (XSS) vulnerability in Code-projects Scholars Tracking System 1.0 allows attackers to run arbitrary code via the News Feed.	5.4	More Details
CVE-2023-50167	Pega Platform from 7.1.7 to 23.1.1 is affected by an XSS issue with editing/rendering user html content.	5.4	More Details
CVE-2024-0561	The Ultimate Posts Widget WordPress plugin before 2.3.1 does not validate and escape some of its Widget options before outputting them back in attributes, 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)	5.4	More Details
CVE-2023-49977	A cross-site scripting (XSS) vulnerability in Customer Support System v1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the address parameter at /customer_support/index.php?page=new_customer.	5.4	More Details
CVE-2024-2406	A vulnerability, which was classified as critical, was found in Gacjie Server up to 1.0. This affects the function index of the file /app/admin/controller/Upload.php. The manipulation of the argument file leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256503.	5.4	More Details
CVE-2024-2245	Cross-Site Scripting vulnerability in moziloCMS version 2.0. By sending a POST request to the '/install.php' endpoint, a JavaScript payload could be executed in the 'username' parameter.	5.4	More Details
CVE-2023-49987	A cross-site scripting (XSS) vulnerability in the component /management/term of School Fees Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the tname parameter.	5.4	More Details
CVE-2023-51281	Cross Site Scripting vulnerability in Customer Support System v.1.0 allows a remote attacker to escalate privileges via a crafted script firstname, "lastname", "middlename", "contact" and address parameters.	5.4	More Details
CVE-2024-2319	Cross-Site Scripting (XSS) vulnerability in the Django MarkdownX project, affecting version 4.0.2. An attacker could store a specially crafted JavaScript payload in the upload functionality due to lack of proper sanitisation of JavaScript elements.	5.4	More Details
CVE-2024-27902	Applications based on SAP GUI for HTML in SAP NetWeaver AS ABAP - versions 7.89, 7.93, do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. A successful attack can allow a malicious attacker to access and modify data through their ability to execute code in a user's browser. There is no impact on the availability of the system	5.4	More Details
CVE-2024-1500	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Logo Widget in all versions up to, and including, 1.3.91 due to insufficient input sanitization and output escaping on user supplied URLs. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33677	Sourcecodester Lost and Found Information System's Version 1.0 is vulnerable to unauthenticated SQL Injection at "?page=items/view&id=*".	5.4	More Details
CVE-2024-28239	Directus is a real-time API and App dashboard for managing SQL database content. The authentication API has a `redirect` parameter that can be exploited as an open redirect vulnerability as the user tries to log in via the API URL. There's a redirect that is done after successful login via the Auth API GET request to `directus/auth/login/google?redirect=http://malicious-fishing-site.com`. While credentials don't seem to be passed to the attacker site, the user can be phished into clicking a legitimate directus site and be taken to a malicious site made to look like a an error message "Your password needs to be updated" to phish out the current password. Users who login via OAuth2 into Directus may be at risk. This issue has been addressed in version 10.10.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.4	More Details
CVE-2024-28216	nGrinder before 3.5.9 allows an attacker to obtain the results of webhook requests due to lack of access control, which could be the cause of information disclosure and limited Server-Side Request Forgery.	5.4	More Details
CVE-2023-49976	A cross-site scripting (XSS) vulnerability in Customer Support System v1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the subject parameter at /customer_support/index.php?page=new_ticket.	5.4	More Details
CVE-2024-25644	Under certain conditions SAP NetWeaver WSRM - version 7.50, allows an attacker to access information which would otherwise be restricted, causing low impact on Confidentiality with no impact on Integrity and Availability of the application.	5.3	More Details
CVE-2024-25645	Under certain condition SAP NetWeaver (Enterprise Portal) - version 7.50 allows an attacker to access information which would otherwise be restricted causing low impact on confidentiality of the application and with no impact on Integrity and Availability of the application.	5.3	More Details
CVE-2024-28163	Under certain conditions, Support Web Pages of SAP NetWeaver Process Integration (PI) - versions 7.50, allows an attacker to access information which would otherwise be restricted, causing low impact on Confidentiality with no impact on Integrity and Availability of the application.	5.3	More Details
CVE-2024-1771	The Total theme for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the total_order_sections() function in all versions up to, and including, 2.1.59. This makes it possible for authenticated attackers, with subscriber-level access and above, to repeat sections on the homepage.	5.3	More Details
CVE-2024-0906	The f(x) Private Site plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.2.1 via the API. This makes it possible for unauthenticated attackers to obtain page and post contents of a site protected with this plugin.	5.3	More Details
CVE-2024-25994	An unauthenticated remote attacker can upload a arbitrary script file due to improper input validation. The upload destination is fixed and is write only.	5.3	More Details
CVE-2024-25996	An unauthenticated remote attacker can perform a remote code execution due to an origin validation error. The access is limited to the service user.	5.3	More Details
CVE-2024-25997	An unauthenticated remote attacker can perform a log injection due to improper input validation. Only a certain log file is affected.	5.3	More Details
CVE-2024-28228	In JetBrains YouTrack before 2024.1.25893 creation comments on behalf of an arbitrary user in HelpDesk was possible	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27305	aiosmtpd is a reimplementation of the Python stdlib smtpd.py based on asyncio. aiosmtpd is vulnerable to inbound SMTP smuggling. SMTP smuggling is a novel vulnerability based on not so novel interpretation differences of the SMTP protocol. By exploiting SMTP smuggling, an attacker may send smuggle/spoof e-mails with fake sender addresses, allowing advanced phishing attacks. This issue is also existed in other SMTP software like Postfix. With the right SMTP server constellation, an attacker can send spoofed e-mails to inbound/receiving aiosmtpd instances. This issue has been addressed in version 1.4.5. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2023-50740	In Apache Linkis <=1.4.0, The password is printed to the log when using the Oracle data source of the Linkis data source module. We recommend users upgrade the version of Linkis to version 1.5.0	5.3	More Details
CVE-2024-28161	In Jenkins Delphix Plugin 3.0.1, a global option for administrators to enable or disable SSL/TLS certificate validation for Data Control Tower (DCT) connections is disabled by default.	5.3	More Details
CVE-2024-26309	Archer Platform 6.x before 6.14 P2 HF2 (6.14.0.2.2) contains a sensitive information disclosure vulnerability. An unauthenticated attacker could potentially obtain access to sensitive information via an internal URL.	5.3	More Details
CVE-2024-22006	OOB read in the TMU plugin that allows for memory disclosure in the power management subsystem of the device.	5.3	More Details
CVE-2023-6444	The Seriously Simple Podcasting WordPress plugin before 3.0.0 discloses the Podcast owner's email address (which by default is the admin email address) via an unauthenticated crafted request.	5.3	More Details
CVE-2024-27938	Postal is an open source SMTP server. Postal versions less than 3.0.0 are vulnerable to SMTP Smuggling attacks which may allow incoming e-mails to be spoofed. This, in conjunction with a cooperative outgoing SMTP service, would allow for an incoming e-mail to be received by Postal addressed from a server that a user has 'authorised' to send mail on their behalf but were not the genuine author of the e-mail. Postal is not affected for sending outgoing e-mails as email is re-encoded with `<CR><LF>` line endings when transmitted over SMTP. This issue has been addressed and users should upgrade to Postal v3.0.0 or higher. Once upgraded, Postal will only accept End of DATA sequences which are explicitly `<CR><LF>.<CR><LF>`. If a non-compliant sequence is detected it will be logged to the SMTP server log. There are no workarounds for this issue.	5.3	More Details
CVE-2024-2265	A vulnerability, which was classified as problematic, was found in keerti1924 PHP-MYSQL-User-Login-System 1.0. This affects an unknown part of the file login.sql. The manipulation leads to inclusion of sensitive information in source code. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256035. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2024-2363	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in AOL AIM Triton 1.0.4. It has been declared as problematic. This vulnerability affects unknown code of the component Invite Handler. The manipulation of the argument CSeq leads to denial of service. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-256318 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	5.3	More Details
CVE-2024-28089	Hitron CODA-4582 2AHKM-CODA4589 7.2.4.5.1b8 devices allow a remote attacker within Wi-Fi proximity (who has access to the router admin panel) to conduct a DOM-based stored XSS attack that can fetch remote resources. The payload is executed at index.html#advanced_location (aka the Device Location page). This can cause a denial of service or lead to information disclosure.	5.2	More Details
CVE-2024-27223	In EUTRAN_LCS_DecodeFacilityInformationElement of LPP_LcsManagement.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure after authenticating the cell connection with no additional execution privileges needed. User interaction is not needed for exploitation.	5.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27230	In ProtocolPsKeepAliveStatusAdapter::getCode() of protocolpsadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with baseband firmware compromise required. User interaction is not needed for exploitation.	5.1	More Details
CVE-2024-21448	Microsoft Teams for Android Information Disclosure Vulnerability	5.0	More Details
CVE-2023-7247	The Login as User or Customer WordPress plugin through 3.8 does not prevent users to log in as any other user on the site.	4.9	More Details
CVE-2023-32969	A cross-site scripting (XSS) vulnerability has been reported to affect Network & Virtual Switch. 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: QuTScloud c5.1.5.2651 and later QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later	4.9	More Details
CVE-2024-28176	jose is JavaScript module for JSON Object Signing and Encryption, providing support for JSON Web Tokens (JWT), JSON Web Signature (JWS), JSON Web Encryption (JWE), JSON Web Key (JWK), JSON Web Key Set (JWKS), and more. A vulnerability has been identified in the JSON Web Encryption (JWE) decryption interfaces, specifically related to the support for decompressing plaintext after its decryption. Under certain conditions it is possible to have the user's environment consume unreasonable amount of CPU time or memory during JWE Decryption operations. This issue has been patched in versions 2.0.7 and 4.15.5.	4.9	More Details
CVE-2024-26005	An unauthenticated remote attacker can gain service level privileges through an incomplete cleanup during service restart after a DoS.	4.8	More Details
CVE-2024-26521	HTML Injection vulnerability in CE Phoenix v1.0.8.20 and before allows a remote attacker to execute arbitrary code, escalate privileges, and obtain sensitive information via a crafted payload to the english.php component.	4.8	More Details
CVE-2023-49971	A cross-site scripting (XSS) vulnerability in Customer Support System v1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the firstname parameter at /customer_support/index.php?page=customer_list.	4.7	More Details
CVE-2024-23235	A race condition was addressed with additional validation. This issue is fixed in macOS Sonoma 14.4, visionOS 1.1, iOS 17.4 and iPadOS 17.4, watchOS 10.4, iOS 16.7.6 and iPadOS 16.7.6, tvOS 17.4. An app may be able to access user-sensitive data.	4.7	More Details
CVE-2024-23275	A race condition was addressed with additional validation. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to access protected user data.	4.7	More Details
CVE-2024-28150	Jenkins HTML Publisher Plugin 1.32 and earlier does not escape job names, report names, and index page titles shown as part of the report frame, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	4.7	More Details
CVE-2024-2394	A vulnerability was found in SourceCodester Employee Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /Admin/add-admin.php. The manipulation of the argument avatar leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-256454 is the identifier assigned to this vulnerability.	4.7	More Details
CVE-2022-46091	Cross Site Scripting (XSS) vulnerability in the feedback form of Online Flight Booking Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the airline parameter.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21901	A SQL injection vulnerability has been reported to affect myQNAPcloud. 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: myQNAPcloud 1.0.52 (2023/11/24) and later QTS 4.5.4.2627 build 20231225 and later	4.7	More Details
CVE-2024-23239	A race condition was addressed with improved state handling. This issue is fixed in tvOS 17.4, iOS 17.4 and iPadOS 17.4, macOS Sonoma 14.4, watchOS 10.4. An app may be able to leak sensitive user information.	4.7	More Details
CVE-2024-2268	A vulnerability was found in keerti1924 Online-Book-Store-Website 1.0. It has been classified as critical. Affected is an unknown function of the file /product_update.php?update=1. The manipulation of the argument update_image leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-256038 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2023-49986	A cross-site scripting (XSS) vulnerability in the component /admin/parent of School Fees Management System 1.0 allow attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the name parameter.	4.7	More Details
CVE-2024-1720	The User Registration – Custom Registration Form, Login Form, and User Profile WordPress Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Display Name' parameter in all versions up to, and including, 3.1.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This vulnerability requires social engineering to successfully exploit, and the impact would be very limited due to the attacker requiring a user to login as the user with the injected payload for execution.	4.7	More Details
CVE-2024-2211	Cross-Site Scripting stored vulnerability in Gophish affecting version 0.12.1. This vulnerability could allow an attacker to store a malicious JavaScript payload in the campaign menu and trigger the payload when the campaign is removed from the menu.	4.6	More Details
CVE-2024-21483	A vulnerability has been identified in SENTRON 7KM PAC3120 AC/DC (7KM3120-0BA01-1DA0) (All versions >= V3.2.3 < V3.2.4 only when manufactured between LQN231003... and LQN231215... (with LQNYYMMDD...)), SENTRON 7KM PAC3120 DC (7KM3120-1BA01-1EA0) (All versions >= V3.2.3 < V3.2.4 only when manufactured between LQN231003... and LQN231215... (with LQNYYMMDD...)), SENTRON 7KM PAC3220 AC/DC (7KM3220-0BA01-1DA0) (All versions >= V3.2.3 < V3.2.4 only when manufactured between LQN231003... and LQN231215... (with LQNYYMMDD...)), SENTRON 7KM PAC3220 DC (7KM3220-1BA01-1EA0) (All versions >= V3.2.3 < V3.2.4 only when manufactured between LQN231003... and LQN231215... (with LQNYYMMDD...)). The read out protection of the internal flash of affected devices was not properly set at the end of the manufacturing process. An attacker with physical access to the device could read out the data.	4.6	More Details
CVE-2024-22133	SAP Fiori Front End Server - version 605, allows altering of approver details on the read-only field when sending leave request information. This could lead to creation of request with incorrect approver causing low impact on Confidentiality and Integrity with no impact on Availability of the application.	4.6	More Details
CVE-2024-23293	This issue was addressed through improved state management. This issue is fixed in tvOS 17.4, iOS 17.4 and iPadOS 17.4, macOS Sonoma 14.4, watchOS 10.4. An attacker with physical access may be able to use Siri to access sensitive user data.	4.6	More Details
CVE-2024-28198	OpenOlat is an open source web-based e-learning platform for teaching, learning, assessment and communication. By manually manipulating http requests when using the draw.io integration it is possible to read arbitrary files as the configured system user and SSRF. The problem is fixed in version 18.1.6 and 18.2.2. It is advised to upgrade to the latest version of 18.1.x or 18.2.x. Users unable to upgrade may work around this issue by disabling the Draw.io module or the entire REST API which will secure the system.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27225	In sendHciCommand of bluetooth_hci.cc, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	4.4	More Details
CVE-2023-52492	In the Linux kernel, the following vulnerability has been resolved: dmaengine: fix NULL pointer in channel unregistration function __dma_async_device_channel_register() can fail. In case of failure, chan->local is freed (with free_percpu()), and chan->local is nullified. When dma_async_device_unregister() is called (because of managed API or intentionally by DMA controller driver), channels are unconditionally unregistered, leading to this NULL pointer: [1.318693] Unable to handle kernel NULL pointer dereference at virtual address 00000000000000d0 [...] [1.484499] Call trace: [1.486930] device_del+0x40/0x394 [1.490314] device_unregister+0x20/0x7c [1.494220] __dma_async_device_channel_unregister+0x68/0xc0 Look at dma_async_device_register() function error path, channel device unregistration is done only if chan->local is not NULL. Then add the same condition at the beginning of __dma_async_device_channel_unregister() function, to avoid NULL pointer issue whatever the API used to reach this function.	4.4	More Details
CVE-2024-20292	A vulnerability in the logging component of Cisco Duo Authentication for Windows Logon and RDP could allow an authenticated, local attacker to view sensitive information in clear text on an affected system. This vulnerability is due to improper storage of an unencrypted registry key in certain logs. An attacker could exploit this vulnerability by accessing the logs on an affected system. A successful exploit could allow the attacker to view sensitive information in clear text.	4.4	More Details
CVE-2024-1443	MSI Afterburner v4.6.5.16370 is vulnerable to a Denial of Service vulnerability by triggering the 0x80002000 IOCTL code of the RTCore64.sys driver. The handle to the driver can only be obtained from a high integrity process.	4.4	More Details
CVE-2024-1400	The Mollie Forms plugin for WordPress is vulnerable to unauthorized post or page duplication due to a missing capability check on the duplicateForm function in all versions up to, and including, 2.6.3. This makes it possible for authenticated attackers, with subscriber access or higher, to duplicate arbitrary posts and pages.	4.3	More Details
CVE-2024-23273	This issue was addressed through improved state management. This issue is fixed in Safari 17.4, iOS 17.4 and iPadOS 17.4, macOS Sonoma 14.4. Private Browsing tabs may be accessed without authentication.	4.3	More Details
CVE-2023-46171	IBM DS8900F HMC 89.21.19.0, 89.21.31.0, 89.30.68.0, 89.32.40.0, and 89.33.48.0 could allow an authenticated user to view sensitive log information after enumerating filenames. IBM X-Force ID: 269408.	4.3	More Details
CVE-2024-21761	An improper authorization vulnerability [CWE-285] in FortiPortal version 7.2.0, and versions 7.0.6 and below reports may allow a user to download other organizations reports via modification in the request payload.	4.3	More Details
CVE-2024-28151	Jenkins HTML Publisher Plugin 1.32 and earlier archives invalid symbolic links in report directories on agents and recreates them on the controller, allowing attackers with Item/Configure permission to determine whether a path on the Jenkins controller file system exists, without being able to access it.	4.3	More Details
CVE-2024-2270	A vulnerability was found in keerti1924 Online-Book-Store-Website 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /signup.php. The manipulation of the argument name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256040. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-2316	A vulnerability has been found in Bdtask Hospital AutoManager up to 20240227 and classified as problematic. This vulnerability affects unknown code of the file /billing/bill/edit/ of the component Update Bill Page. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-256270 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28158	A cross-site request forgery (CSRF) vulnerability in Jenkins Subversion Partial Release Manager Plugin 1.0.1 and earlier allows attackers to trigger a build.	4.3	More Details
CVE-2024-1645	The Mollie Forms plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the exportRegistrations function in all versions up to, and including, 2.6.3. This makes it possible for authenticated attackers, with subscriber access or higher, to export payment data collected by this plugin.	4.3	More Details
CVE-2024-28159	A missing permission check in Jenkins Subversion Partial Release Manager Plugin 1.0.1 and earlier allows attackers with Item/Read permission to trigger a build.	4.3	More Details
CVE-2024-27900	Due to missing authorization check, attacker with business user account in SAP ABAP Platform - version 758, 795, can change the privacy setting of job templates from shared to private. As a result, the selected template would only be accessible to the owner.	4.3	More Details
CVE-2024-28173	In JetBrains TeamCity between 2023.11 and 2023.11.4 custom build parameters of the "password" type could be disclosed	4.3	More Details
CVE-2024-2277	A vulnerability was found in Bdtask G-Prescription Gynaecology & OBS Consultation Software 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /Setting/change_password_save of the component Password Reset Handler. The manipulation leads to cross-site request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-256046 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-2298	The affiliate-toolkit – WordPress Affiliate Plugin plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the atkp_import_product() function in all versions up to, and including, 3.5.4. This makes it possible for authenticated attackers, with subscriber-level access and above, to to perform unauthorized actions such as creating importing products.	4.3	More Details
CVE-2024-26167	Microsoft Edge for Android Spoofing Vulnerability	4.3	More Details
CVE-2024-2318	A vulnerability was found in ZKTeco ZKBio Media 2.0.0_x64_2024-01-29-1028. It has been classified as problematic. Affected is an unknown function of the file /pro/common/download of the component Service Port 9999. The manipulation of the argument fileName with the input ../../../../zkbio_media.sql leads to path traversal: '../filedir'. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256272. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-28180	Package jose aims to provide an implementation of the Javascript Object Signing and Encryption set of standards. An attacker could send a JWE containing compressed data that used large amounts of memory and CPU when decompressed by Decrypt or DecryptMulti. Those functions now return an error if the decompressed data would exceed 250kB or 10x the compressed size (whichever is larger). This vulnerability has been patched in versions 4.0.1, 3.0.3 and 2.6.3.	4.3	More Details
CVE-2023-4626	The LadiApp plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the ladiflow_save_hook() function in versions up to, and including, 4.3. This makes it possible for authenticated attackers with subscriber-level access and above to update the 'ladiflow_hook_configs' option.	4.3	More Details
CVE-2023-4627	The LadiApp plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the save_config() function in versions up to, and including, 4.4. This makes it possible for authenticated attackers with subscriber-level access and above to update the 'ladipage_config' option.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4628	The LadiApp plugin for WordPress is vulnerable to Cross-Site Request Forgery due to a missing nonce check on the ladiflow_save_hook() function in versions up to, and including, 4.4. This makes it possible for unauthenticated attackers to update the 'ladiflow_hook_configs' option 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-2024-22256	VMware Cloud Director contains a partial information disclosure vulnerability. A malicious actor can potentially gather information about organization names based on the behavior of the instance.	4.3	More Details
CVE-2023-4728	The LadiApp plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the publish_lp() function hooked via an AJAX action in versions up to, and including, 4.4. This makes it possible for authenticated attackers with subscriber-level access and above to change the LadiPage key (a key fully controlled by the attacker), enabling them to freely create new pages, including web pages that trigger stored XSS	4.3	More Details
CVE-2023-4729	The LadiApp plugin for WordPress is vulnerable to Cross-Site Request Forgery due to a missing nonce check on the publish_lp() function hooked via an AJAX action in versions up to, and including, 4.4. This makes it possible for unauthenticated attackers to change the LadiPage key (a key fully controlled by the attacker), enabling them to freely create new pages, including web pages that trigger stored XSS 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-2023-4731	The LadiApp plugn for WordPress is vulnerable to Cross-Site Request Forgery due to a missing nonce check on the init_endpoint() function hooked via 'init' in versions up to, and including, 4.4. This makes it possible for unauthenticated attackers to modify a variety of settings, via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. An attacker can directly modify the 'ladipage_key' which enables them to create new posts on the website and inject malicious web scripts,	4.3	More Details
CVE-2024-1760	The Appointment Booking Calendar — Simply Schedule Appointments Booking Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.6.6.20. This is due to missing or incorrect nonce validation on the ssa_factory_reset() function. This makes it possible for unauthenticated attackers to reset the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2024-1124	The EventPrime – Events Calendar, Bookings and Tickets plugin for WordPress is vulnerable to unauthorized email sending due to a missing capability check on the ep_send_attendees_email() function in all versions up to, and including, 3.4.1. This makes it possible for authenticated attackers, with subscriber-level access and above, to send arbitrary emails with arbitrary content from the site.	4.3	More Details
CVE-2024-2267	A vulnerability was found in keerti1924 Online-Book-Store-Website 1.0 and classified as problematic. This issue affects some unknown processing of the file /shop.php. The manipulation of the argument product_price leads to business logic errors. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256037 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-1870	The Colibri Page Builder plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the callActivateLicenseEndpoint function in all versions up to, and including, 1.0.260. This makes it possible for authenticated attackers, with subscriber access or higher, to update the license key.	4.3	More Details
CVE-2024-1137	The Proxy and Client components of TIBCO Software Inc.'s TIBCO ActiveSpaces - Enterprise Edition contain a vulnerability that theoretically allows an Active Spaces client to passively observe data traffic to other clients. Affected releases are TIBCO Software Inc.'s TIBCO ActiveSpaces - Enterprise Edition: versions 4.4.0 through 4.9.0.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21900	An 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 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTScloud c5.1.5.2651 and later	4.3	More Details
CVE-2024-2354	A vulnerability, which was classified as problematic, was found in Dreamer CMS 4.1.3. Affected is an unknown function of the file /admin/menu/toEdit. The manipulation of the argument id leads to cross-site request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-256314 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-27707	Server Side Request Forgery (SSRF) vulnerability in hcengineering Huly Platform v.0.6.202 allows attackers to run arbitrary code via upload of crafted SVG file.	4.3	More Details
CVE-2023-4629	The LadiApp plugin for WordPress is vulnerable to Cross-Site Request Forgery due to a missing nonce check on the save_config() function in versions up to, and including, 4.3. This makes it possible for unauthenticated attackers to update the 'ladipage_config' option 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-2024-28162	In Jenkins Delphix Plugin 3.0.1 through 3.1.0 (both inclusive) a global option for administrators to enable or disable SSL/TLS certificate validation for Data Control Tower (DCT) connections fails to take effect until Jenkins is restarted when switching from disabled validation to enabled validation.	4.2	More Details
CVE-2023-52597	In the Linux kernel, the following vulnerability has been resolved: KVM: s390: fix setting of fpc register kvm_arch_vcpu_ioctl_set_fpu() allows to set the floating point control (fpc) register of a guest cpu. The new value is tested for validity by temporarily loading it into the fpc register. This may lead to corruption of the fpc register of the host process: if an interrupt happens while the value is temporarily loaded into the fpc register, and within interrupt context floating point or vector registers are used, the current fp/vx registers are saved with save_fpu_regs() assuming they belong to user space and will be loaded into fp/vx registers when returning to user space. test_fp_ctl() restores the original user space / host process fpc register value, however it will be discarded, when returning to user space. In result the host process will incorrectly continue to run with the value that was supposed to be used for a guest cpu. Fix this by simply removing the test. There is another test right before the SIE context is entered which will handles invalid values. This results in a change of behaviour: invalid values will now be accepted instead of that the ioctl fails with -EINVAL. This seems to be acceptable, given that this interface is most likely not used anymore, and this is in addition the same behaviour implemented with the memory mapped interface (replace invalid values with zero) - see sync_regs() in kvm-s390.c.	4.0	More Details
CVE-2024-2317	A vulnerability was found in Bdtask Hospital AutoManager up to 20240227 and classified as problematic. This issue affects some unknown processing of the file /prescription/prescription/delete/ of the component Prescription Page. The manipulation leads to improper authorization. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256271. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.8	More Details
CVE-2023-52584	In the Linux kernel, the following vulnerability has been resolved: spmi: mediatek: Fix UAF on device remove The pmif driver data that contains the clocks is allocated along with spmi_controller. On device remove, spmi_controller will be freed first, and then devres , including the clocks, will be cleanup. This leads to UAF because putting the clocks will access the clocks in the pmif driver data, which is already freed along with spmi_controller. This can be reproduced by enabling DEBUG_TEST_DRIVER_REMOVE and building the kernel with KASAN. Fix the UAF issue by using unmanaged clk_bulk_get() and putting the clocks before freeing spmi_controller.	3.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1410	Cloudflare quiche was discovered to be vulnerable to unbounded storage of information related to connection ID retirement, which could lead to excessive resource consumption. Each QUIC connection possesses a set of connection Identifiers (IDs); see RFC 9000 Section 5.1 https://datatracker.ietf.org/doc/html/rfc9000#section-5.1 . Endpoints declare the number of active connection IDs they are willing to support using the active_connection_id_limit transport parameter. The peer can create new IDs using a NEW_CONNECTION_ID frame but must stay within the active ID limit. This is done by retirement of old IDs, the endpoint sends NEW_CONNECTION_ID includes a value in the retire_prior_to field, which elicits a RETIRE_CONNECTION_ID frame as confirmation. An unauthenticated remote attacker can exploit the vulnerability by sending NEW_CONNECTION_ID frames and manipulating the connection (e.g. by restricting the peer's congestion window size) so that RETIRE_CONNECTION_ID frames can only be sent at a slower rate than they are received, leading to storage of information related to connection IDs in an unbounded queue. Quiche versions 0.19.2 and 0.20.1 are the earliest to address this problem. There is no workaround for affected versions.	3.7	More Details
CVE-2024-2355	A vulnerability has been found in keerti1924 Secret-Coder-PHP-Project 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /secret_coder.sql. The manipulation leads to inclusion of sensitive information in source code. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256315. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2024-2284	A vulnerability classified as problematic was found in boyiddha Automated-Mess-Management-System 1.0. Affected by this vulnerability is an unknown functionality of the file /member/chat.php of the component Chat Book. The manipulation of the argument msg leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256051. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-2285	A vulnerability, which was classified as problematic, has been found in boyiddha Automated-Mess-Management-System 1.0. Affected by this issue is some unknown functionality of the file /member/member_edit.php. The manipulation of the argument name leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-256052. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-2266	A vulnerability has been found in keerti1924 Secret-Coder-PHP-Project 1.0 and classified as problematic. This vulnerability affects unknown code of the file /login.php of the component Login Page. The manipulation of the argument emailcookie/passwordcookie leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256036. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-28113	Peering Manager is a BGP session management tool. In Peering Manager <=1.8.2, it is possible to redirect users to an arbitrary page using a crafted url. As a result users can be redirected to an unexpected location. This issue has been addressed in version 1.8.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.	3.5	More Details
CVE-2024-0053	In getCustomPrinterIcon of PrintManagerService.java, there is a possible way to view other user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2024-23253	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.4. An app may be able to access a user's Photos Library.	3.3	More Details
CVE-2024-23257	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.7.4, macOS Ventura 13.6.5, macOS Sonoma 14.4, visionOS 1.1, iOS 16.7.6 and iPadOS 16.7.6. Processing an image may result in disclosure of process memory.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23262	This issue was addressed with additional entitlement checks. This issue is fixed in visionOS 1.1, iOS 17.4 and iPadOS 17.4, iOS 16.7.6 and iPadOS 16.7.6. An app may be able to spoof system notifications and UI.	3.3	More Details
CVE-2024-23232	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sonoma 14.4. An app may be able to capture a user's screen.	3.3	More Details
CVE-2024-23227	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to read sensitive location information.	3.3	More Details
CVE-2024-23245	This issue was addressed by adding an additional prompt for user consent. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. Third-party shortcuts may use a legacy action from Automator to send events to apps without user consent.	3.3	More Details
CVE-2024-0052	In multiple functions of healthconnect, there is a possible leakage of exercise route data due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2024-25991	In acpm_tmu_ipc_handler of tmu_plugin.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2024-23289	A lock screen issue was addressed with improved state management. This issue is fixed in iOS 16.7.6 and iPadOS 16.7.6, iOS 17.4 and iPadOS 17.4, macOS Sonoma 14.4, watchOS 10.4. A person with physical access to a device may be able to use Siri to access private calendar information.	3.3	More Details
CVE-2024-23291	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in tvOS 17.4, iOS 17.4 and iPadOS 17.4, macOS Sonoma 14.4, watchOS 10.4. A malicious app may be able to observe user data in log entries related to accessibility notifications.	3.3	More Details
CVE-2024-23292	This issue was addressed with improved data protection. This issue is fixed in macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4. An app may be able to access information about a user's contacts.	3.3	More Details
CVE-2024-23242	A privacy issue was addressed by not logging contents of text fields. This issue is fixed in macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4. An app may be able to view Mail data.	3.3	More Details
CVE-2024-23238	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Sonoma 14.4. An app may be able to edit NVRAM variables.	3.3	More Details
CVE-2024-2313	If kernel headers need to be extracted, bpftrace will attempt to load them from a temporary directory. An unprivileged attacker could use this to force bcc to load compromised linux headers. Linux distributions which provide kernel headers by default are not affected by default.	2.8	More Details
CVE-2024-2314	If kernel headers need to be extracted, bcc will attempt to load them from a temporary directory. An unprivileged attacker could use this to force bcc to load compromised linux headers. Linux distributions which provide kernel headers by default are not affected by default.	2.8	More Details
CVE-2022-46498	Hospital Management System 1.0 was discovered to contain a SQL injection vulnerability via the doc_number parameter at his_admin_view_single_employee.php.	2.7	More Details
CVE-2024-28214	nGrinder before 3.5.9 allows to set delay without limitation, which could be the cause of Denial of Service by remote attacker.	2.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25114	Collabora Online is a collaborative online office suite based on LibreOffice technology. Each document in Collabora Online is opened by a separate "Kit" instance in a different "jail" with a unique directory "jailID" name. For security reasons, this directory name is randomly generated and should not be given out to the client. In affected versions of Collabora Online it is possible to use the CELL() function, with the "filename" argument, in the spreadsheet component to get a path which includes this JailID. The impact of this vulnerability in its own is low because it requires to be chained with another vulnerability. Users should upgrade to Collabora Online 23.05.9; Collabora Online 22.05.22; Collabora Online 21.11.10 or higher. There are no known workarounds for this vulnerability.	2.6	More Details
CVE-2024-23255	An authentication issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4. Photos in the Hidden Photos Album may be viewed without authentication.	2.4	More Details
CVE-2024-2276	A vulnerability has been found in Bdtask G-Prescription Gynaecology & OBS Consultation Software 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /Venue_controller/edit_venue/ of the component Edit Venue Page. The manipulation of the argument Venue map leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256045 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2024-2274	A vulnerability, which was classified as problematic, has been found in Bdtask G-Prescription Gynaecology & OBS Consultation Software 1.0. This issue affects some unknown processing of the file /Home/Index of the component Prescription Dashboard. The manipulation of the argument Title leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256043. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2024-23240	The issue was addressed with improved checks. This issue is fixed in iOS 17.4 and iPadOS 17.4. Shake-to-undo may allow a deleted photo to be re-surfaced without authentication.	2.4	More Details
CVE-2024-2275	A vulnerability, which was classified as problematic, was found in Bdtask G-Prescription Gynaecology & OBS Consultation Software 1.0. Affected is an unknown function of the component OBS Patient/Gynee Prescription. The manipulation of the argument Patient Title/Full Name/Address/Cheif Complain/LMP/Menstrual Edd/OBS P/OBS Alc/Medicine Name/Medicine Type/Ml/Dose/Days/Comments/Template 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. The identifier of this vulnerability is VDB-256044. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2024-2391	A vulnerability was found in EVE-NG 5.0.1-13 and classified as problematic. Affected by this issue is some unknown functionality of the component Lab Handler. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-256442 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2024-28238	Directus is a real-time API and App dashboard for managing SQL database content. When reaching the /files page, a JWT is passed via GET request. Inclusion of session tokens in URLs poses a security risk as URLs are often logged in various places (e.g., web server logs, browser history). Attackers gaining access to these logs may hijack active user sessions, leading to unauthorized access to sensitive information or actions on behalf of the user. This issue has been addressed in version 10.10.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2.3	More Details
CVE-2024-2364	A vulnerability classified as problematic has been found in Musicshelf 1.0/1.1 on Android. Affected is an unknown function of the file androidmanifest.xml of the component Backup Handler. The manipulation leads to exposure of backup file to an unauthorized control sphere. It is possible to launch the attack on the physical device. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256320.	1.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2365	A vulnerability classified as problematic was found in Musicshelf 1.0/1.1 on Android. Affected by this vulnerability is an unknown functionality of the file io\fabric\sdk\android\services\network\PinningTrustManager.java of the component SHA-1 Handler. The manipulation leads to password hash with insufficient computational effort. It is possible to launch the attack on the physical device. 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 identifier VDB-256321 was assigned to this vulnerability.	1.6	More Details
CVE-2023-52490	In the Linux kernel, the following vulnerability has been resolved: mm: migrate: fix getting incorrect page mapping during page migration When running stress-ng testing, we found below kernel crash after a few hours: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 pc : dentry_name+0xd8/0x224 lr : pointer+0x22c/0x370 sp : ffff800025f134c0 ..... Call trace: dentry_name+0xd8/0x224 pointer+0x22c/0x370 vsnprintf+0x1ec/0x730 vscnprintf+0x2c/0x60 vprintk_store+0x70/0x234 vprintk_emit+0xe0/0x24c vprintk_default+0x3c/0x44 vprintk_func+0x84/0x2d0 printk+0x64/0x88 __dump_page+0x52c/0x530 dump_page+0x14/0x20 set_migratetype_isolate+0x110/0x224 start_isolate_page_range+0xc4/0x20c offline_pages+0x124/0x474 memory_block_offline+0x44/0xf4 memory_subsys_offline+0x3c/0x70 device_offline+0xf0/0x120 ..... After analyzing the vmcore, I found this issue is caused by page migration. The scenario is that, one thread is doing page migration, and we will use the target page's ->mapping field to save 'anon_vma' pointer between page unmap and page move, and now the target page is locked and refcount is 1. Currently, there is another stress-ng thread performing memory hotplug, attempting to offline the target page that is being migrated. It discovers that the refcount of this target page is 1, preventing the offline operation, thus proceeding to dump the page. However, page_mapping() of the target page may return an incorrect file mapping to crash the system in dump_mapping(), since the target page->mapping only saves 'anon_vma' pointer without setting PAGE_MAPPING_ANON flag. There are seveval ways to fix this issue: (1) Setting the PAGE_MAPPING_ANON flag for target page's ->mapping when saving 'anon_vma', but this can confuse PageAnon() for PFN walkers, since the target page has not built mappings yet. (2) Getting the page lock to call page_mapping() in __dump_page() to avoid crashing the system, however, there are still some PFN walkers that call page_mapping() without holding the page lock, such as compaction. (3) Using target page->private field to save the 'anon_vma' pointer and 2 bits page state, just as page->mapping records an anonymous page, which can remove the page_mapping() impact for PFN walkers and also seems a simple way. So I choose option 3 to fix this issue, and this can also fix other potential issues for PFN walkers, such as compaction.	N/A	More Details
CVE-2024-23252	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-0917	remote code execution in paddlepaddle/paddle 2.6.0	N/A	More Details
CVE-2024-27218	In update_freq_data of , there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52489	In the Linux kernel, the following vulnerability has been resolved: mm/sparsemem: fix race in accessing memory_section->usage The below race is observed on a PFN which falls into the device memory region with the system memory configuration where PFN's are such that [ZONE_NORMAL ZONE_DEVICE ZONE_NORMAL]. Since normal zone start and end pfn contains the device memory PFN's as well, the compaction triggered will try on the device memory PFN's too though they end up in NOP(because pfn_to_online_page() returns NULL for ZONE_DEVICE memory sections). When from other core, the section mappings are being removed for the ZONE_DEVICE region, that the PFN in question belongs to, on which compaction is currently being operated is resulting into the kernel crash with CONFIG_SPASEMEM_VMEMAP enabled. The crash logs can be seen at [1]. compact_zone() memunmap_pages ------------ ---------- __pageblock_pfn_to_page ..... (a)pfn_valid(): valid_section()//return true (b)__remove_pages()-> sparse_remove_section()-> section_deactivate(): [Free the array ms->usage and set ms->usage = NULL] pfn_section_valid() [Access ms->usage which is NULL] NOTE: From the above it can be said that the race is reduced to between the pfn_valid()/pfn_section_valid() and the section deactivate with SPASEMEM_VMEMAP enabled. The commit b943f045a9af("mm/sparse: fix kernel crash with pfn_section_valid check") tried to address the same problem by clearing the SECTION_HAS_MEM_MAP with the expectation of valid_section() returns false thus ms->usage is not accessed. Fix this issue by the below steps: a) Clear SECTION_HAS_MEM_MAP before freeing the ->usage. b) RCU protected read side critical section will either return NULL when SECTION_HAS_MEM_MAP is cleared or can successfully access ->usage. c) Free the ->usage with kfree_rcu() and set ms->usage = NULL. No attempt will be made to access ->usage after this as the SECTION_HAS_MEM_MAP is cleared thus valid_section() return false. Thanks to David/Pavan for their inputs on this patch. [1] https://lore.kernel.org/linux-mm/994410bb-89aa-d987-1f50-f514903c55aa@quicinc.com/ On Snapdragon SoC, with the mentioned memory configuration of PFN's as [ZONE_NORMAL ZONE_DEVICE ZONE_NORMAL], we are able to see bunch of issues daily while testing on a device farm. For this particular issue below is the log. Though the below log is not directly pointing to the pfn_section_valid(){ ms->usage;}, when we loaded this dump on T32 lauterbach tool, it is pointing. [540.578056] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 [540.578068] Mem abort info: [540.578070] ESR = 0x0000000096000005 [540.578073] EC = 0x25: DABT (current EL), IL = 32 bits [540.578077] SET = 0, FnV = 0 [540.578080] EA = 0, S1PTW = 0 [540.578082] FSC = 0x05: level 1 translation fault [540.578085] Data abort info: [540.578086] ISV = 0, ISS = 0x00000005 [540.578088] CM = 0, WnR = 0 [540.579431] pstate: 82400005 (Nzcv daif +PAN -UAO +TCO -DIT -SSBSBTYPE=--) [540.579436] pc : __pageblock_pfn_to_page+0x6c/0x14c [540.579454] lr : compact_zone+0x994/0x1058 [540.579460] sp : ffffffc03579b510 [540.579463] x29: ffffffc03579b510 x28: 0000000000235800 x27:000000000000000c [540.579470] x26: 0000000000235c00 x25: 0000000000000068 x24:ffffffc03579b640 [540.579477] x23: 0000000000000001 x22: ffffffc03579b660 x21:0000000000000000 [540.579483] x20: 0000000000235bff x19: ffffffdebf7e3940 x18:ffffffdebf66d140 [540.579489] x17: 00000000739ba063 x16: 00000000739ba063 x15:00000000009f4bff [540.579495] x14: 0000008000000000 x13: 0000000000000000 x12:0000000000000001 [540.579501] x11: 0000000000000000 x10: 0000000000000000 x9 :ffffff897d2cd440 [540.579507] x8 : 0000000000000000 x7 : 0000000000000000 x6 :ffffffc03579b5b4 [540.579512] x5 : 0000000000027f25 x4 : ffffffc03579b5b8 x3 :0000000000000 ---truncated---	N/A	More Details
CVE-2023-52583	In the Linux kernel, the following vulnerability has been resolved: ceph: fix deadlock or deadcode of misusing dget() The lock order is incorrect between denty and its parent, we should always make sure that the parent get the lock first. But since this deadcode is never used and the parent dir will always be set from the callers, let's just remove it.	N/A	More Details
CVE-2023-41014	code-projects.org Online Job Portal 1.0 is vulnerable to SQL Injection via the Username parameter for "Employer."	N/A	More Details
CVE-2024-26613	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42307	Cross Site Scripting (XSS) vulnerability in Code-Projects Exam Form Submission 1.0 allows attackers to run arbitrary code via "Subject Name" and "Subject Code" section.	N/A	More Details
CVE-2023-52494	In the Linux kernel, the following vulnerability has been resolved: bus: mhi: host: Add alignment check for event ring read pointer Though we do check the event ring read pointer by "is_valid_ring_ptr" to make sure it is in the buffer range, but there is another risk the pointer may be not aligned. Since we are expecting event ring elements are 128 bits(struct mhi_ring_element) aligned, an unaligned read pointer could lead to multiple issues like DoS or ring buffer memory corruption. So add a alignment check for event ring read pointer.	N/A	More Details
CVE-2024-0818	Arbitrary File Overwrite Via Path Traversal in paddlepaddle/paddle before 2.6	N/A	More Details
CVE-2023-52495	In the Linux kernel, the following vulnerability has been resolved: soc: qcom: pmic_glink_altmode: fix port sanity check The PMIC GLINK altmode driver currently supports at most two ports. Fix the incomplete port sanity check on notifications to avoid accessing and corrupting memory beyond the port array if we ever get a notification for an unsupported port.	N/A	More Details
CVE-2024-27698	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2024-27227	A malicious DNS response can trigger a number of OOB reads, writes, and other memory issues	N/A	More Details
CVE-2024-27229	In ss_SendCallBarringPwdRequiredIndMsg of ss_CallBarring.c, there is a possible null pointer deref due to a missing null check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2024-26609	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-47691	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-52496	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-27237	In wipe_ns_memory of nsmemwipe.c, there is a possible incorrect size calculation due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2024-21584	Pleasanter 1.3.49.0 and earlier contains a cross-site scripting vulnerability. If an attacker tricks the user to access the product with a specially crafted URL and perform a specific operation, an arbitrary script may be executed on the web browser of the user.	N/A	More Details
CVE-2024-24101	Code-projects Scholars Tracking System 1.0 is vulnerable to SQL Injection under Eligibility Information Update.	N/A	More Details
CVE-2024-27613	Numbas editor before 7.3 mishandles reading of themes and extensions.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27278	OpenPNE Plugin "opTimelinePlugin" 1.2.11 and earlier contains a cross-site scripting vulnerability. On the site which uses the affected product, when a user configures the profile with some malicious contents, an arbitrary script may be executed on the web browsers of other users.	N/A	More Details
CVE-2024-0559	The Enhanced Text Widget WordPress plugin before 1.6.6 does not validate and escape some of its Widget options before outputting them back in attributes, 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)	N/A	More Details
CVE-2024-1487	The Photos and Files Contest Gallery WordPress plugin before 21.3.1 does not sanitize and escape some parameters, which could allow users with a role as low as author to perform Cross-Site Scripting attacks.	N/A	More Details
CVE-2024-0817	Command injection in IrGraph.draw in paddlepaddle/paddle 2.6.0	N/A	More Details
CVE-2023-52587	In the Linux kernel, the following vulnerability has been resolved: IB/ipoib: Fix mcast list locking Releasing the `priv->lock` while iterating the `priv->multicast_list` in `ipoib_mcast_join_task()` opens a window for `ipoib_mcast_dev_flush()` to remove the items while in the middle of iteration. If the mcast is removed while the lock was dropped, the for loop spins forever resulting in a hard lockup (as was reported on RHEL 4.18.0-372.75.1.el8_6 kernel): Task A (kworker/u72:2 below) I Task B (kworker/u72:0 below) ---------- ipoib_mcast_join_task(work) I ipoib_ib_dev_flush_light(work) spin_lock_irq(&priv->lock) I __ipoib_ib_dev_flush(priv, ...) list_for_each_entry(mcast, I ipoib_mcast_dev_flush(dev = priv->dev) &priv->multicast_list, list) I ipoib_mcast_join(dev, mcast) I spin_unlock_irq(&priv->lock) I I spin_lock_irqsave(&priv->lock, flags) I list_for_each_entry_safe(mcast, tmcast, I &priv->multicast_list, list) I list_del(&mcast->list); I list_add_tail(&mcast->list, &remove_list) I spin_unlock_irqrestore(&priv->lock, flags) spin_lock_irq(&priv->lock) I I ipoib_mcast_remove_list(&remove_list) (Here, `mcast` is no longer on the I list_for_each_entry_safe(mcast, tmcast, `priv->multicast_list` and we keep I remove_list, list) spinning on the `remove_list` of I >>> wait_for_completion(&mcast->done) the other thread which is blocked I and the list is still valid on I it's stack.) Fix this by keeping the lock held and changing to GFP_ATOMIC to prevent eventual sleeps. Unfortunately we could not reproduce the lockup and confirm this fix but based on the code review I think this fix should address such lockups. crash> bc 31 PID: 747 TASK: ff1c6a1a007e8000 CPU: 31 COMMAND: "kworker/u72:2" -- [exception RIP: ipoib_mcast_join_task+0x1b1] RIP: ffffffffc0944ac1 RSP: ff646f199a8c7e00 RFLAGS: 00000002 RAX: 0000000000000000 RBX: ff1c6a1a04dc82f8 RCX: 0000000000000000 work (&priv->mcast_task{,.work}) RDX: ff1c6a192d60ac68 RSI: 0000000000000286 RDI: ff1c6a1a04dc8000 &mcast->list RBP: ff646f199a8c7e90 R8: ff1c699980019420 R9: ff1c6a1920c9a000 R10: ff646f199a8c7e00 R11: ff1c6a191a7d9800 R12: ff1c6a192d60ac00 mcast R13: ff1c6a1d82200000 R14: ff1c6a1a04dc8000 R15: ff1c6a1a04dc82d8 dev priv (&priv->lock) &priv->multicast_list (aka head) ORIG_RAX: ffffffffffffffff CS: 0010 SS: 0018 --- <NMI exception stack> --- #5 [ff646f199a8c7e00] ipoib_mcast_join_task+0x1b1 at ffffffffc0944ac1 [ib_ipoib] #6 [ff646f199a8c7e98] process_one_work+0x1a7 at ffffffff9bf10967 crash> rx ff646f199a8c7e68 ff646f199a8c7e68: ff1c6a1a04dc82f8 <<< work = &priv->mcast_task.work crash> list -hO ipoib_dev_priv.multicast_list ff1c6a1a04dc8000 (empty) crash> ipoib_dev_priv.mcast_task.work.func,mcast_mutex.owner.counter ff1c6a1a04dc8000 mcast_task.work.func = 0xffffffffc0944910 <ipoib_mcast_join_task>, mcast_mutex.owner.counter = 0xff1c69998efec000 crash> b 8 PID: 8 TASK: ff1c69998efec000 CPU: 33 COMMAND: "kworker/u72:0" -- #3 [ff646f1980153d50] wait_for_completion+0x96 at ffffffff9c7d7646 #4 [ff646f1980153d90] ipoib_mcast_remove_list+0x56 at ffffffffc0944dc6 [ib_ipoib] #5 [ff646f1980153de8] ipoib_mcast_dev_flush+0x1a7 at ffffffffc09455a7 [ib_ipoib] #6 [ff646f1980153e58] __ipoib_ib_dev_flush+0x1a4 at ffffffffc09431a4 [ib_ipoib] #7 [ff ---truncated---	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52586	In the Linux kernel, the following vulnerability has been resolved: drm/msm/dpu: Add mutex lock in control vblank irq Add a mutex lock to control vblank irq to synchronize vblank enable/disable operations happening from different threads to prevent race conditions while registering/unregistering the vblank irq callback. v4: -Removed vblank_ctl_lock from dpu_encoder_virt, so it is only a parameter of dpu_encoder_phys. -Switch from atomic refcnt to a simple int counter as mutex has now been added v3: Mistakenly did not change wording in last version. It is done now. v2: Slightly changed wording of commit message Patchwork: https://patchwork.freedesktop.org/patch/571854/	N/A	More Details
CVE-2024-26618	In the Linux kernel, the following vulnerability has been resolved: arm64/sme: Always exit sme_alloc() early with existing storage When sme_alloc() is called with existing storage and we are not flushing we will always allocate new storage, both leaking the existing storage and corrupting the state. Fix this by separating the checks for flushing and for existing storage as we do for SVE. Callers that reallocate (eg, due to changing the vector length) should call sme_free() themselves.	N/A	More Details
CVE-2023-52486	In the Linux kernel, the following vulnerability has been resolved: drm: Don't unref the same fb many times by mistake due to deadlock handling If we get a deadlock after the fb lookup in drm_mode_page_flip_ioctl() we proceed to unref the fb and then retry the whole thing from the top. But we forget to reset the fb pointer back to NULL, and so if we then get another error during the retry, before the fb lookup, we proceed the unref the same fb again without having gotten another reference. The end result is that the fb will (eventually) end up being freed while it's still in use. Reset fb to NULL once we've unreffed it to avoid doing it again until we've done another fb lookup. This turned out to be pretty easy to hit on a DG2 when doing async flips (and CONFIG_DEBUG_WW_MUTEX_SLOWPATH=y). The first symptom I saw that drm_closefb() simply got stuck in a busy loop while walking the framebuffer list. Fortunately I was able to convince it to oops instead, and from there it was easier to track down the culprit.	N/A	More Details
CVE-2024-26620	In the Linux kernel, the following vulnerability has been resolved: s390/vfio-ap: always filter entire AP matrix The vfio_ap_mdev_filter_matrix function is called whenever a new adapter or domain is assigned to the mdev. The purpose of the function is to update the guest's AP configuration by filtering the matrix of adapters and domains assigned to the mdev. When an adapter or domain is assigned, only the APQNs associated with the APID of the new adapter or APQI of the new domain are inspected. If an APQN does not reference a queue device bound to the vfio_ap device driver, then it's APID will be filtered from the mdev's matrix when updating the guest's AP configuration. Inspecting only the APID of the new adapter or APQI of the new domain will result in passing AP queues through to a guest that are not bound to the vfio_ap device driver under certain circumstances. Consider the following: guest's AP configuration (all also assigned to the mdev's matrix): 14.0004 14.0005 14.0006 16.0004 16.0005 16.0006 unassign domain 4 unbind queue 16.0005 assign domain 4 When domain 4 is re-assigned, since only domain 4 will be inspected, the APQNs that will be examined will be: 14.0004 16.0004 Since both of those APQNs reference queue devices that are bound to the vfio_ap device driver, nothing will get filtered from the mdev's matrix when updating the guest's AP configuration. Consequently, queue 16.0005 will get passed through despite not being bound to the driver. This violates the linux device model requirement that a guest shall only be given access to devices bound to the device driver facilitating their pass-through. To resolve this problem, every adapter and domain assigned to the mdev will be inspected when filtering the mdev's matrix.	N/A	More Details
CVE-2023-4780	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-0590. Reason: This candidate is a duplicate of CVE-2024-0590. Notes: All CVE users should reference CVE-2024-0590 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-28153	Jenkins OWASP Dependency-Check Plugin 5.4.5 and earlier does not escape vulnerability metadata from Dependency-Check reports, resulting in a stored cross-site scripting (XSS) vulnerability.	N/A	More Details
CVE-2024-2370	Rejected reason: DO NOT USE THIS CVE ID NUMBER. Consult IDs: CVE-2018-5341. Reason: This CVE Record is a duplicate of CVE-2018-5341. Notes: All CVE users should reference CVE-2018-5341 instead of this record.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22011	In ss_ProcessRejectComponent of ss_MmConManagement.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2024-26628	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-1373	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-46209. Reason: This candidate is a duplicate of CVE-2023-46209. Notes: All CVE users should reference CVE-2023-46209 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-28816	Student Information Chatbot a0196ab allows SQL injection via the username to the login function in index.php.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26625	In the Linux kernel, the following vulnerability has been resolved: llc: call sock_orphan() at release time syzbot reported an interesting trace [1] caused by a stale sk->sk_wq pointer in a closed llc socket. In commit ff7b11aa481f ("net: socket: set sock->sk to NULL after calling proto_ops::release()") Eric Biggers hinted that some protocols are missing a sock_orphan(), we need to perform a full audit. In net-next, I plan to clear sock->sk from sock_orphan() and amend Eric patch to add a warning. [1] BUG: KASAN: slab-use-after-free in list_empty include/linux/list.h:373 [inline] BUG: KASAN: slab-use-after-free in waitqueue_active include/linux/wait.h:127 [inline] BUG: KASAN: slab-use-after-free in sock_def_write_space_wfree net/core/sock.c:3384 [inline] BUG: KASAN: slab-use-after-free in sock_wfree+0x9a8/0x9d0 net/core/sock.c:2468 Read of size 8 at addr ffff88802f4fc880 by task ksoftirqd/1/27 CPU: 1 PID: 27 Comm: ksoftirqd/1 Not tainted 6.8.0-rc1-syzkaller-00049-g6098d87eaf31 #0 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.2-debian-1.16.2-1 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xd9/0x1b0 lib/dump_stack.c:106 print_address_description mm/kasan/report.c:377 [inline] print_report+0xc4/0x620 mm/kasan/report.c:488 kasan_report+0xda/0x110 mm/kasan/report.c:601 list_empty include/linux/list.h:373 [inline] waitqueue_active include/linux/wait.h:127 [inline] sock_def_write_space_wfree net/core/sock.c:3384 [inline] sock_wfree+0x9a8/0x9d0 net/core/sock.c:2468 skb_release_head_state+0xa3/0x2b0 net/core/skbuff.c:1080 skb_release_all net/core/skbuff.c:1092 [inline] napi_consume_skb+0x119/0x2b0 net/core/skbuff.c:1404 e1000_unmap_and_free_tx_resource+0x144/0x200 drivers/net/ethernet/intel/e1000/e1000_main.c:1970 e1000_clean_tx_irq drivers/net/ethernet/intel/e1000/e1000_main.c:3860 [inline] e1000_clean+0x4a1/0x26e0 drivers/net/ethernet/intel/e1000/e1000_main.c:3801 __napi_poll.constprop.0+0xb4/0x540 net/core/dev.c:6576 napi_poll net/core/dev.c:6645 [inline] net_rx_action+0x956/0xe90 net/core/dev.c:6778 __do_softirq+0x21a/0x8de kernel/softirq.c:553 run_ksoftirqd kernel/softirq.c:921 [inline] run_ksoftirqd+0x31/0x60 kernel/softirq.c:913 smpboot_thread_fn+0x660/0xa10 kernel/smpboot.c:164 kthread+0x2c6/0x3a0 kernel/kthread.c:388 ret_from_fork+0x45/0x80 arch/x86/kernel/process.c:147 ret_from_fork_asm+0x11/0x20 arch/x86/entry/entry_64.S:242 </TASK> Allocated by task 5167: kasan_save_stack+0x33/0x50 mm/kasan/common.c:47 kasan_save_track+0x14/0x30 mm/kasan/common.c:68 unpoison_slab_object mm/kasan/common.c:314 [inline] __kasan_slab_alloc+0x81/0x90 mm/kasan/common.c:340 kasan_slab_alloc include/linux/kasan.h:201 [inline] slab_post_alloc_hook mm/slub.c:3813 [inline] slab_alloc_node mm/slub.c:3860 [inline] kmem_cache_alloc_lru+0x142/0x6f0 mm/slub.c:3879 alloc_inode_sb include/linux/fs.h:3019 [inline] sock_alloc_inode+0x25/0x1c0 net/socket.c:308 alloc_inode+0x5d/0x220 fs/inode.c:260 new_inode_pseudo+0x16/0x80 fs/inode.c:1005 sock_alloc+0x40/0x270 net/socket.c:634 __sock_create+0xbc/0x800 net/socket.c:1535 sock_create net/socket.c:1622 [inline] __sys_socket_create net/socket.c:1659 [inline] __sys_socket+0x14c/0x260 net/socket.c:1706 __do_sys_socket net/socket.c:1720 [inline] __se_sys_socket net/socket.c:1718 [inline] __x64_sys_socket+0x72/0xb0 net/socket.c:1718 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xd3/0x250 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b Freed by task 0: kasan_save_stack+0x33/0x50 mm/kasan/common.c:47 kasan_save_track+0x14/0x30 mm/kasan/common.c:68 kasan_save_free_info+0x3f/0x60 mm/kasan/generic.c:640 poison_slab_object mm/kasan/common.c:241 [inline] __kasan_slab_free+0x121/0x1b0 mm/kasan/common.c:257 kasan_slab_free include/linux/kasan.h:184 [inline] slab_free_hook mm/slub.c:2121 [inlin ---truncated---	N/A	More Details
CVE-2024-26624	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-28154	Jenkins MQ Notifier Plugin 1.4.0 and earlier logs potentially sensitive build parameters as part of debug information in build logs by default.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26623	In the Linux kernel, the following vulnerability has been resolved: pds_core: Prevent race issues involving the adminq There are multiple paths that can result in using the pdsc's adminq. [1] pdsc_adminq_isr and the resulting work from queue_work(), i.e. pdsc_work_thread()->pdsc_process_adminq() [2] pdsc_adminq_post() When the device goes through reset via PCIe reset and/or a fw_down/fw_up cycle due to bad PCIe state or bad device state the adminq is destroyed and recreated. A NULL pointer dereference can happen if [1] or [2] happens after the adminq is already destroyed. In order to fix this, add some further state checks and implement reference counting for adminq uses. Reference counting was used because multiple threads can attempt to access the adminq at the same time via [1] or [2]. Additionally, multiple clients (i.e. pds-vfio-pci) can be using [2] at the same time. The adminq_refcnt is initialized to 1 when the adminq has been allocated and is ready to use. Users/clients of the adminq (i.e. [1] and [2]) will increment the refcnt when they are using the adminq. When the driver goes into a fw_down cycle it will set the PDSC_S_FW_DEAD bit and then wait for the adminq_refcnt to hit 1. Setting the PDSC_S_FW_DEAD before waiting will prevent any further adminq_refcnt increments. Waiting for the adminq_refcnt to hit 1 allows for any current users of the adminq to finish before the driver frees the adminq. Once the adminq_refcnt hits 1 the driver clears the refcnt to signify that the adminq is deleted and cannot be used. On the fw_up cycle the driver will once again initialize the adminq_refcnt to 1 allowing the adminq to be used again.	N/A	More Details
CVE-2024-28155	Jenkins AppSpider Plugin 1.0.16 and earlier does not perform permission checks in several HTTP endpoints, allowing attackers with Overall/Read permission to obtain information about available scan config names, engine group names, and client names.	N/A	More Details
CVE-2023-52606	In the Linux kernel, the following vulnerability has been resolved: powerpc/lib: Validate size for vector operations Some of the fp/vmx code in sstep.c assume a certain maximum size for the instructions being emulated. The size of those operations however is determined separately in analyse_instr(). Add a check to validate the assumption on the maximum size of the operations, so as to prevent any unintended kernel stack corruption.	N/A	More Details
CVE-2024-1279	The Paid Memberships Pro WordPress plugin before 2.12.9 does not prevent user with at least the contributor role from leaking other users' sensitive metadata.	N/A	More Details
CVE-2023-52598	In the Linux kernel, the following vulnerability has been resolved: s390/ptrace: handle setting of fpc register correctly If the content of the floating point control (fpc) register of a traced process is modified with the ptrace interface the new value is tested for validity by temporarily loading it into the fpc register. This may lead to corruption of the fpc register of the tracing process: if an interrupt happens while the value is temporarily loaded into the fpc register, and within interrupt context floating point or vector registers are used, the current fp/vx registers are saved with save_fpu_regs() assuming they belong to user space and will be loaded into fp/vx registers when returning to user space. test_fp_ctl() restores the original user space fpc register value, however it will be discarded, when returning to user space. In result the tracer will incorrectly continue to run with the value that was supposed to be used for the traced process. Fix this by saving fpu register contents with save_fpu_regs() before using test_fp_ctl().	N/A	More Details
CVE-2024-28156	Jenkins Build Monitor View Plugin 1.14-860.vd06ef2568b_3f and earlier does not escape Build Monitor View names, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to configure Build Monitor Views.	N/A	More Details
CVE-2023-52596	In the Linux kernel, the following vulnerability has been resolved: sysctl: Fix out of bounds access for empty sysctl registers When registering tables to the sysctl subsystem there is a check to see if header is a permanently empty directory (used for mounts). This check evaluates the first element of the ctl_table. This results in an out of bounds evaluation when registering empty directories. The function register_sysctl_mount_point now passes a ctl_table of size 1 instead of size 0. It now relies solely on the type to identify a permanently empty register. Make sure that the ctl_table has at least one element before testing for permanent emptiness.	N/A	More Details
CVE-2024-0815	Command injection in paddle.utils.download._wget_download (bypass filter) in paddlepaddle/paddle 2.6.0	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52592	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-52590	In the Linux kernel, the following vulnerability has been resolved: ocfs2: Avoid touching renamed directory if parent does not change The VFS will not be locking moved directory if its parent does not change. Change ocfs2 rename code to avoid touching renamed directory if its parent does not change as without locking that can corrupt the filesystem.	N/A	More Details
CVE-2023-52589	In the Linux kernel, the following vulnerability has been resolved: media: rkisp1: Fix IRQ disable race issue In rkisp1_isp_stop() and rkisp1_csi_disable() the driver masks the interrupts and then apparently assumes that the interrupt handler won't be running, and proceeds in the stop procedure. This is not the case, as the interrupt handler can already be running, which would lead to the ISP being disabled while the interrupt handler handling a captured frame. This brings up two issues: 1) the ISP could be powered off while the interrupt handler is still running and accessing registers, leading to board lockup, and 2) the interrupt handler code and the code that disables the streaming might do things that conflict. It is not clear to me if 2) causes a real issue, but 1) can be seen with a suitable delay (or printk in my case) in the interrupt handler, leading to board lockup.	N/A	More Details
CVE-2023-52488	In the Linux kernel, the following vulnerability has been resolved: serial: sc16is7xx: convert from _raw_ to _noinc_ regmap functions for FIFO The SC16IS7XX IC supports a burst mode to access the FIFOs where the initial register address is sent ($00), followed by all the FIFO data without having to resend the register address each time. In this mode, the IC doesn't increment the register address for each R/W byte. The regmap_raw_read() and regmap_raw_write() are functions which can perform IO over multiple registers. They are currently used to read/write from/to the FIFO, and although they operate correctly in this burst mode on the SPI bus, they would corrupt the regmap cache if it was not disabled manually. The reason is that when the R/W size is more than 1 byte, these functions assume that the register address is incremented and handle the cache accordingly. Convert FIFO R/W functions to use the regmap _noinc_ versions in order to remove the manual cache control which was a workaround when using the _raw_ versions. FIFO registers are properly declared as volatile so cache will not be used/updated for FIFO accesses.	N/A	More Details
CVE-2023-52588	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to tag gcing flag on page during block migration It needs to add missing gcing flag on page during block migration, in order to garantee migrated data be persisted during checkpoint, otherwise out-of-order persistency between data and node may cause data corruption after SPOR. Similar issue was fixed by commit 2d1fe8a86bf5 ("f2fs: fix to tag gcing flag on page during file defragment").	N/A	More Details
CVE-2024-24389	A cross-site scripting (XSS) vulnerability in XunRuiCMS up to v4.6.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Add Column Name parameter.	N/A	More Details
CVE-2024-28757	libexpat through 2.6.1 allows an XML Entity Expansion attack when there is isolated use of external parsers (created via XML_ExternalEntityParserCreate).	N/A	More Details
CVE-2023-52605	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details