SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 05 June 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-2024-3820	The wpDataTables – WordPress Data Table, Dynamic Tables & Table Charts Plugin plugin for WordPress is vulnerable to SQL Injection via the 'id_key' parameter of the wdt_delete_table_row AJAX action in all versions up to, and including, 6.3.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Please note this only affects the premium version of the plugin.	10.0	More Details
CVE-2024-36388	MileSight DeviceHub - CWE-305 Missing Authentication for Critical Function	10.0	More Details
CVE-2024-25600	Improper Control of Generation of Code ('Code Injection') vulnerability in Codeer Limited Bricks Builder allows Code Injection.This issue affects Bricks Builder: from n/a through 1.9.6.	10.0	More Details
CVE-2024-3200	The wpForo Forum plugin for WordPress is vulnerable to SQL Injection via the 'slug' attribute of the 'wpforo' shortcode in all versions up to, and including, 2.3.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	9.9	More Details
CVE-2024-31682	Incorrect access control in the fingerprint authentication mechanism of Phone Cleaner: Boost & Clean v2.2.0 allows attackers to bypass fingerprint authentication due to the use of a deprecated API.	9.8	More Details
CVE-2024-27776	MileSight DeviceHub - CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') may allow Unauthenticated RCE	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36389	MileSight DeviceHub - CWE-330 Use of Insufficiently Random Values may allow Authentication Bypass	9.8	More Details
CVE-2024-36042	Silverpeas before 6.3.5 allows authentication bypass by omitting the Password field to AuthenticationServlet, often providing an unauthenticated user with superadmin access.	9.8	More Details
CVE-2024-5311	DigiWin EasyFlow .NET lacks validation for certain input parameters. An unauthenticated remote attacker can inject arbitrary SQL commands to read, modify, and delete database records.	9.8	More Details
CVE-2024-5404	An unauthenticated remote attacker can change the admin password in a moneo appliance due to weak password recovery mechanism.	9.8	More Details
CVE-2024-36568	Sourcecodester Gas Agency Management System v1.0 is vulnerable to SQL Injection via /gasmark/editbrand.php?id=.	9.8	More Details
CVE-2024-37019	Northern.tech Mender Enterprise before 3.6.4 and 3.7.x before 3.7.4 has Weak Authentication.	9.8	More Details
CVE-2024-5150	The Login with phone number plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 1.7.26. This is due to the 'activation_code' default value is empty, and the not empty check is missing in the 'lwp_ajax_register' function. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the user email. The vulnerability is patched in version 1.7.26, but there is an issue in the patch that causes the entire function to not work, and this issue is fixed in version 1.7.27.	9.8	More Details
CVE-2024-36783	TOTOLINK LR350 V9.3.5u.6369_B20220309 was discovered to contain a command injection via the host_time parameter in the NTPSyncWithHost function.	9.8	More Details
CVE-2024-29972	** UNSUPPORTED WHEN ASSIGNED ** The command injection vulnerability in the CGI program "remote_help-cgi" in Zyxel NAS326 firmware versions before V5.21(AAZF.17)C0 and NAS542 firmware versions before V5.21(ABAG.14)C0 could allow an unauthenticated attacker to execute some operating system (OS) commands by sending a crafted HTTP POST request.	9.8	More Details
CVE-2024-29973	** UNSUPPORTED WHEN ASSIGNED ** The command injection vulnerability in the “setCookie” parameter in Zyxel NAS326 firmware versions before V5.21(AAZF.17)C0 and NAS542 firmware versions before V5.21(ABAG.14)C0 could allow an unauthenticated attacker to execute some operating system (OS) commands by sending a crafted HTTP POST request.	9.8	More Details
CVE-2024-29974	** UNSUPPORTED WHEN ASSIGNED ** The remote code execution vulnerability in the CGI program “file_upload-cgi” in Zyxel NAS326 firmware versions before V5.21(AAZF.17)C0 and NAS542 firmware versions before V5.21(ABAG.14)C0 could allow an unauthenticated attacker to execute arbitrary code by uploading a crafted configuration file to a vulnerable device.	9.8	More Details
CVE-2024-4552	The Social Login Lite For WooCommerce plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 1.6.0. This is due to insufficient verification on the user being supplied during the social login through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email.	9.8	More Details
CVE-2024-35700	Improper Privilege Management vulnerability in DeluxeThemes Userpro allows Privilege Escalation.This issue affects Userpro: from n/a through 5.1.8.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36604	Tenda O3V2 v1.0.0.12(3880) was discovered to contain a Blind Command Injection via stpEn parameter in the SetStp function. This vulnerability allows attackers to execute arbitrary commands with root privileges.	9.8	More Details
CVE-2024-36858	An arbitrary file upload vulnerability in the /v1/app/writeFileSync interface of Jan v0.4.12 allows attackers to execute arbitrary code via uploading a crafted file.	9.8	More Details
CVE-2024-37273	An arbitrary file upload vulnerability in the /v1/app/appendFileSync interface of Jan v0.4.12 allows attackers to execute arbitrary code via uploading a crafted file.	9.8	More Details
CVE-2024-36782	TOTOLINK CP300 V2.0.4-B20201102 was discovered to contain a hardcoded password vulnerability in /etc/shadow.sample, which allows attackers to log in as root.	9.8	More Details
CVE-2024-20067	In modem, there is a possible out of bounds write due to improper input invalidation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01267285; Issue ID: MSV-1462.	9.8	More Details
CVE-2024-33999	The referrer URL used by MFA required additional sanitizing, rather than being used directly.	9.8	More Details
CVE-2024-35469	A SQL injection vulnerability in /hrm/user/ in SourceCodester Human Resource Management System 1.0 allows attackers to execute arbitrary SQL commands via the password parameter.	9.8	More Details
CVE-2024-4358	In Progress Telerik Report Server, version 2024 Q1 (10.0.24.305) or earlier, on IIS, an unauthenticated attacker can gain access to Telerik Report Server restricted functionality via an authentication bypass vulnerability.	9.8	More Details
CVE-2024-5514	MinMax CMS from MinMax Digital Technology contains a hidden administrator account with a fixed password that cannot be removed or disabled from the management interface. Remote attackers who obtain this account can bypass IP access control restrictions and log in to the backend system without being recorded in the system logs.	9.8	More Details
CVE-2024-1100	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Vadi Corporate Information Systems DIGIKENT GIS allows SQL Injection.This issue affects DIGIKENT GIS: through 2.23.5.	9.8	More Details
CVE-2024-35354	A vulnerability has been discovered in Diño Physics School Assistant version 2.3. The vulnerability impacts an unidentified code within the file /classes/Master.php?f=save_category. Manipulating the argument id can result in SQL injection.	9.8	More Details
CVE-2024-35355	A vulnerability has been discovered in Diño Physics School Assistant version 2.3. The vulnerability impacts an unidentified code within the file /classes/Master.php?f=delete_category. Manipulating the argument id can result in SQL injection.	9.8	More Details
CVE-2024-36031	In the Linux kernel, the following vulnerability has been resolved: keys: Fix overwrite of key expiration on instantiation The expiry time of a key is unconditionally overwritten during instantiation, defaulting to turn it permanent. This causes a problem for DNS resolution as the expiration set by user-space is overwritten to TIME64_MAX, disabling further DNS updates. Fix this by restoring the condition that key_set_expiry is only called when the pre-parser sets a specific expiry.	9.8	More Details
CVE-2024-35350	A vulnerability has been discovered in Diño Physics School Assistant version 2.3. The vulnerability impacts an unidentified code within the file /admin/?page=borrow/view_borrow. Manipulating the argument id can result in SQL injection.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35353	A vulnerability has been discovered in Diño Physics School Assistant version 2.3. The vulnerability impacts an unidentified code within the file /classes/Users.php?f=save. Manipulating the argument id can result in improper authorization.	9.8	More Details
CVE-2024-35359	A vulnerability has been discovered in Diño Physics School Assistant version 2.3. The vulnerability impacts an unidentified code within the file /classes/Master.php?f=view_item. Manipulating the argument id can result in SQL injection.	9.8	More Details
CVE-2024-35349	A vulnerability has been discovered in Diño Physics School Assistant version 2.3. The vulnerability impacts an unidentified code within the file /admin/category/view_category.php. Manipulating the argument id can result in SQL injection.	9.8	More Details
CVE-2024-36108	casgate is an Open Source Identity and Access Management system. In affected versions `casgate` allows remote unauthenticated attacker to obtain sensitive information via GET request to an API endpoint. This issue has been addressed in PR #201 which is pending merge. An attacker could use `id` parameter of GET requests with value `anonymous/ anonymous` to bypass authorization on certain API endpoints. Successful exploitation of the vulnerability could lead to account takeover, privilege escalation or provide attacker with credential to other services. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.8	More Details
CVE-2024-23692	Rejetto HTTP File Server, up to and including version 2.3m, is vulnerable to a template injection vulnerability. This vulnerability allows a remote, unauthenticated attacker to execute arbitrary commands on the affected system by sending a specially crafted HTTP request. As of the CVE assignment date, Rejetto HFS 2.3m is no longer supported.	9.8	More Details
CVE-2024-32850	Improper neutralization of special elements used in a command ('Command Injection') exists in SkyBridge MB-A100/MB-A110 firmware Ver. 4.2.2 and earlier and SkyBridge BASIC MB-A130 firmware Ver. 1.5.5 and earlier. If the remote monitoring and control function is enabled on the product, an attacker with access to the product may execute an arbitrary command or login to the product with the administrator privilege.	9.8	More Details
CVE-2024-36246	Missing authorization vulnerability exists in Unifier and Unifier Cast Version.5.0 or later, and the patch "20240527" not applied. If this vulnerability is exploited, arbitrary code may be executed with LocalSystem privilege. As a result, a malicious program may be installed, data may be modified or deleted.	9.8	More Details
CVE-2024-35629	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Wow-Company Easy Digital Downloads – Recent Purchases allows PHP Remote File Inclusion.This issue affects Easy Digital Downloads – Recent Purchases: from n/a through 1.0.2.	9.6	More Details
CVE-2024-36400	nano-id is a unique string ID generator for Rust. Affected versions of the nano-id crate incorrectly generated IDs using a reduced character set in the `nano_id::base62` and `nano_id::base58` functions. Specifically, the `base62` function used a character set of 32 symbols instead of the intended 62 symbols, and the `base58` function used a character set of 16 symbols instead of the intended 58 symbols. Additionally, the `nano_id::gen` macro is also affected when a custom character set that is not a power of 2 in size is specified. It should be noted that `nano_id::base64` is not affected by this vulnerability. This can result in a significant reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0.	9.4	More Details
CVE-2023-43556	Memory corruption in Hypervisor when platform information mentioned is not aligned.	9.3	More Details
CVE-2023-43538	Memory corruption in TZ Secure OS while Tunnel Invoke Manager initialization.	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3050	The Site Reviews WordPress plugin before 7.0.0 retrieves client IP addresses from potentially untrusted headers, allowing an attacker to manipulate its value. This may be used to bypass IP-based blocking	9.1	More Details
CVE-2024-3412	The WP STAGING WordPress Backup Plugin – Migration Backup Restore plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the wpstg_processing AJAX action in all versions up to, and including, 3.4.3. This makes it possible for authenticated attackers, with administrator-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.1	More Details
CVE-2024-36391	MileSight DeviceHub - CWE-320: Key Management Errors may allow Authentication Bypass and Man-In-The-Middle Traffic	9.1	More Details
CVE-2024-34792	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in dexta Dextaz Ping allows Command Injection.This issue affects Dextaz Ping: from n/a through 0.65.	9.1	More Details
CVE-2024-36104	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 18.12.14. Users are recommended to upgrade to version 18.12.14, which fixes the issue.	9.1	More Details
CVE-2023-43551	Cryptographic issue while performing attach with a LTE network, a rogue base station can skip the authentication phase and immediately send the Security Mode Command.	9.1	More Details
CVE-2023-33930	Unrestricted Upload of File with Dangerous Type vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates) allows Code Injection.This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 1.5.66.	9.1	More Details
CVE-2024-36896	In the Linux kernel, the following vulnerability has been resolved: USB: core: Fix access violation during port device removal Testing with KASAN and syzkaller revealed a bug in port.c:disable_store(): usb_hub_to_struct_hub() can return NULL if the hub that the port belongs to is concurrently removed, but the function does not check for this possibility before dereferencing the returned value. It turns out that the first dereference is unnecessary, since hub->intfdev is the parent of the port device, so it can be changed easily. Adding a check for hub == NULL prevents further problems. The same bug exists in the disable_show() routine, and it can be fixed the same way.	9.1	More Details
CVE-2024-31030	An issue in coap_msg.c in Keith Cullen's FreeCoAP v.0.7 allows remote attackers to cause a Denial of Service or potentially disclose information via a specially crafted packet.	9.1	More Details
CVE-2024-37018	The OpenDaylight 0.15.3 controller allows topology poisoning via API requests because an application can manipulate the path that is taken by discovery packets.	9.1	More Details
CVE-2024-34987	A SQL Injection vulnerability exists in the `ofrs/admin/index.php` script of PHPGurukul Online Fire Reporting System 1.2. The vulnerability allows attackers to bypass authentication and gain unauthorized access by injecting SQL commands into the username input field during the login process.	9.1	More Details
CVE-2024-36675	LyLme_spage v1.9.5 is vulnerable to Server-Side Request Forgery (SSRF) via the get_head function.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33560	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in 8theme XStore allows PHP Local File Inclusion.This issue affects XStore: from n/a through 9.3.8.	9.0	More Details
CVE-2024-34551	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Select-Themes Stockholm allows PHP Local File Inclusion.This issue affects Stockholm: from n/a through 9.6.	9.0	More Details
CVE-2024-3300	An unsafe .NET object deserialization vulnerability in DELMIA Apriso Release 2019 through Release 2024 could lead to pre-authentication remote code execution.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-5499	Out of bounds write in Streams API in Google Chrome prior to 125.0.6422.141 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-5496	Use after free in Media Session in Google Chrome prior to 125.0.6422.141 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-29825	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an unauthenticated attacker within the same network to execute arbitrary code.	8.8	More Details
CVE-2024-29824	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an unauthenticated attacker within the same network to execute arbitrary code.	8.8	More Details
CVE-2024-37061	Remote Code Execution can occur in versions of the MLflow platform running version 1.11.0 or newer, enabling a maliciously crafted MLproject to execute arbitrary code on an end user's system when run.	8.8	More Details
CVE-2024-29822	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an unauthenticated attacker within the same network to execute arbitrary code.	8.8	More Details
CVE-2024-33628	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in XforWooCommerce allows PHP Local File Inclusion.This issue affects XforWooCommerce: from n/a through 2.0.2.	8.8	More Details
CVE-2024-5523	SQL injection vulnerability in Astrotalks affecting version 10/03/2023. This vulnerability could allow an authenticated local user to send a specially crafted SQL query to the 'searchString' parameter and retrieve all information stored in the database.	8.8	More Details
CVE-2024-5326	The Post Grid Gutenberg Blocks and WordPress Blog Plugin – PostX plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'postx_presets_callback' function in all versions up to, and including, 4.1.2. This makes it possible for authenticated attackers, with Contributor-level access and above, to change arbitrary options on affected sites. This can be used to enable new user registration and set the default role for new users to Administrator.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5345	The Responsive Owl Carousel for Elementor plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.2.0 via the layout parameter. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included. The inclusion is limited to PHP files.	8.8	More Details
CVE-2024-5498	Use after free in Presentation API in Google Chrome prior to 125.0.6422.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-5497	Out of bounds memory access in Browser UI in Google Chrome prior to 125.0.6422.141 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-5495	Use after free in Dawn in Google Chrome prior to 125.0.6422.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-29827	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an unauthenticated attacker within the same network to execute arbitrary code.	8.8	More Details
CVE-2024-5494	Use after free in Dawn in Google Chrome prior to 125.0.6422.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-5493	Heap buffer overflow in WebRTC in Google Chrome prior to 125.0.6422.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-37052	Deserialization of untrusted data can occur in versions of the MLflow platform running version 1.1.0 or newer, enabling a maliciously uploaded scikit-learn model to run arbitrary code on an end user’s system when interacted with.	8.8	More Details
CVE-2024-37053	Deserialization of untrusted data can occur in versions of the MLflow platform running version 1.1.0 or newer, enabling a maliciously uploaded scikit-learn model to run arbitrary code on an end user’s system when interacted with.	8.8	More Details
CVE-2024-37054	Deserialization of untrusted data can occur in versions of the MLflow platform running version 0.9.0 or newer, enabling a maliciously uploaded PyFunc model to run arbitrary code on an end user’s system when interacted with.	8.8	More Details
CVE-2024-37055	Deserialization of untrusted data can occur in versions of the MLflow platform running version 1.24.0 or newer, enabling a maliciously uploaded pmdarima model to run arbitrary code on an end user’s system when interacted with.	8.8	More Details
CVE-2024-37056	Deserialization of untrusted data can occur in versions of the MLflow platform running version 1.23.0 or newer, enabling a maliciously uploaded LightGBM scikit-learn model to run arbitrary code on an end user’s system when interacted with.	8.8	More Details
CVE-2024-37057	Deserialization of untrusted data can occur in versions of the MLflow platform running version 2.0.0rc0 or newer, enabling a maliciously uploaded Tensorflow model to run arbitrary code on an end user’s system when interacted with.	8.8	More Details
CVE-2024-37058	Deserialization of untrusted data can occur in versions of the MLflow platform running version 2.5.0 or newer, enabling a maliciously uploaded Langchain AgentExecutor model to run arbitrary code on an end user’s system when interacted with.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37059	Deserialization of untrusted data can occur in versions of the MLflow platform running version 0.5.0 or newer, enabling a maliciously uploaded PyTorch model to run arbitrary code on an end user's system when interacted with.	8.8	More Details
CVE-2024-29826	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an unauthenticated attacker within the same network to execute arbitrary code.	8.8	More Details
CVE-2024-29823	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an unauthenticated attacker within the same network to execute arbitrary code.	8.8	More Details
CVE-2024-37060	Deserialization of untrusted data can occur in versions of the MLflow platform running version 1.27.0 or newer, enabling a maliciously crafted Recipe to execute arbitrary code on an end user's system when run.	8.8	More Details
CVE-2024-5348	The Elements For Elementor plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.1 via the 'beforeafter_layout' attribute of the beforeafter widget, the 'eventsgrid_layout' attribute of the eventsgrid and list widgets, the 'marquee_layout' attribute of the marquee widget, the 'postgrid_layout' attribute of the postgrid widget, the 'woocart_layout' attribute of the woocart widget, and the 'woogrid_layout' attribute of the woogrid widget. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included.	8.8	More Details
CVE-2023-6743	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.5.89 via the template import functionality. This makes it possible for authenticated attackers, with contributor access and above, to execute code on the server.	8.8	More Details
CVE-2024-36547	idccms V1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component admin/vpsClass_deal.php?mudi=add	8.8	More Details
CVE-2024-36550	idccms V1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via /admin/vpsCompany_deal.php?mudi=add&nohrefStr=close	8.8	More Details
CVE-2024-36549	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via /admin/vpsCompany_deal.php?mudi=rev&nohrefStr=close	8.8	More Details
CVE-2024-5204	The Swiss Toolkit For WP plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 1.0.7. This is due to the plugin storing custom data in post metadata without an underscore prefix. This makes it possible for authenticated attackers with contributor-level and above permissions to log in as any existing user on the site, such as an administrator.	8.8	More Details
CVE-2024-23668	An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and 6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI.	8.8	More Details
CVE-2024-34007	The logout option within MFA did not include the necessary token to avoid the risk of users inadvertently being logged out via CSRF.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34008	Actions in the admin management of analytics models did not include the necessary token to prevent a CSRF risk.	8.8	More Details
CVE-2024-36548	idccms V1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via admin/vpsCompany_deal.php?mudi=del	8.8	More Details
CVE-2024-28826	Improper restriction of local upload and download paths in check_sftp in Checkmk before 2.3.0p4, 2.2.0p27, 2.1.0p44, and in Checkmk 2.0.0 (EOL) allows attackers with sufficient permissions to configure the check to read and write local files on the Checkmk site server.	8.8	More Details
CVE-2024-3564	The Content Blocks (Custom Post Widget) plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 3.3.0 via the plugin's 'content_block' shortcode. This makes it possible for authenticated attackers, with contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included.	8.8	More Details
CVE-2024-36114	Aircompressor is a library with ports of the Snappy, LZO, LZ4, and Zstandard compression algorithms to Java. All decompressor implementations of Aircompressor (LZ4, LZO, Snappy, Zstandard) can crash the JVM for certain input, and in some cases also leak the content of other memory of the Java process (which could contain sensitive information). When decompressing certain data, the decompressors try to access memory outside the bounds of the given byte arrays or byte buffers. Because Aircompressor uses the JDK class `sun.misc.Unsafe` to speed up memory access, no additional bounds checks are performed and this has similar security consequences as out-of-bounds access in C or C++, namely it can lead to non-deterministic behavior or crash the JVM. Users should update to Aircompressor 0.27 or newer where these issues have been fixed. When decompressing data from untrusted users, this can be exploited for a denial-of-service attack by crashing the JVM, or to leak other sensitive information from the Java process. There are no known workarounds for this issue.	8.6	More Details
CVE-2024-3301	An unsafe .NET object deserialization vulnerability in DELMIA Apriso Release 2019 through Release 2024 could lead to post-authentication remote code execution.	8.5	More Details
CVE-2024-33557	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in 8theme XStore Core allows PHP Local File Inclusion.This issue affects XStore Core: from n/a through 5.3.8.	8.5	More Details
CVE-2024-34554	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Select-Themes Stockholm Core allows PHP Local File Inclusion.This issue affects Stockholm Core: from n/a through 2.4.1.	8.5	More Details
CVE-2024-34552	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Select-Themes Stockholm allows PHP Local File Inclusion.This issue affects Stockholm: from n/a through 9.6.	8.5	More Details
CVE-2024-33568	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Deserialization of Untrusted Data vulnerability in BdThemes Element Pack Pro allows Path Traversal, Object Injection.This issue affects Element Pack Pro: from n/a through 7.7.4.	8.5	More Details
CVE-2022-0555	Subiquity Shows Guided Storage Passphrase in Plaintext with Read-all Permissions	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23360	Memory corruption while creating a LPAC client as LPAC engine was allowed to access GPU registers.	8.4	More Details
CVE-2024-35142	IBM Security Verify Access Docker 10.0.0 through 10.0.6 could allow a local user to escalate their privileges due to execution of unnecessary privileges. IBM X-Force ID: 292418.	8.4	More Details
CVE-2024-35333	A stack-buffer-overflow vulnerability exists in the read_charset_decl function of html2xhtml 1.3. This vulnerability occurs due to improper bounds checking when copying data into a fixed-size stack buffer. An attacker can exploit this vulnerability by providing a specially crafted input to the vulnerable function, causing a buffer overflow and potentially leading to arbitrary code execution, denial of service, or data corruption.	8.4	More Details
CVE-2024-34001	Actions in the admin preset tool did not include the necessary token to prevent a CSRF risk.	8.4	More Details
CVE-2023-47837	Improper Privilege Management vulnerability in Repute Infosystems ARMember allows Privilege Escalation.This issue affects ARMember: from n/a through 4.0.10.	8.3	More Details
CVE-2024-5525	Improper privilege management vulnerability in Astrotalks affecting version 10/03/2023. This vulnerability allows a local user to access the application as an administrator without any provided credentials, allowing the attacker to perform administrative actions.	8.3	More Details
CVE-2024-4749	The wp-eMember WordPress plugin before 10.3.9 does not sanitize and escape the "fieldId" parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting.	8.3	More Details
CVE-2024-21512	Versions of the package mysql2 before 3.9.8 are vulnerable to Prototype Pollution due to improper user input sanitization passed to fields and tables when using nestTables.	8.2	More Details
CVE-2023-43555	Information disclosure in Video while parsing mp2 clip with invalid section length.	8.2	More Details
CVE-2024-32983	Misskey is an open source, decentralized microblogging platform. Misskey doesn't perform proper normalization on the JSON structures of incoming signed ActivityPub activity objects before processing them, allowing threat actors to spoof the contents of signed activities and impersonate the authors of the original activities. This vulnerability is fixed in 2024.5.0.	8.2	More Details
CVE-2024-36267	Path traversal vulnerability exists in Redmine DMSF Plugin versions prior to 3.1.4. If this vulnerability is exploited, a logged-in user may obtain or delete arbitrary files on the server (within the privilege of the Redmine process).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36886	In the Linux kernel, the following vulnerability has been resolved: tipc: fix UAF in error path Sam Page (sam4k) working with Trend Micro Zero Day Initiative reported a UAF in the tipc_buf_append() error path: BUG: KASAN: slab-use-after-free in kfree_skb_list_reason+0x47e/0x4c0 linux/net/core/skbuff.c:1183 Read of size 8 at addr ffff88804d2a7c80 by task poc/8034 CPU: 1 PID: 8034 Comm: poc Not tainted 6.8.2 #1 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.0-debian-1.16.0-5 04/01/2014 Call Trace: <IRQ> __dump_stack linux/lib/dump_stack.c:88 dump_stack_lvl+0xd9/0x1b0 linux/lib/dump_stack.c:106 print_address_description linux/mm/kasan/report.c:377 print_report+0xc4/0x620 linux/mm/kasan/report.c:488 kasan_report+0xda/0x110 linux/mm/kasan/report.c:601 kfree_skb_list_reason+0x47e/0x4c0 linux/net/core/skbuff.c:1183 skb_release_data+0x5af/0x880 linux/net/core/skbuff.c:1026 skb_release_all linux/net/core/skbuff.c:1094 __kfree_skb linux/net/core/skbuff.c:1108 kfree_skb_reason+0x12d/0x210 linux/net/core/skbuff.c:1144 kfree_skb linux/./include/linux/skbuff.h:1244 tipc_buf_append+0x425/0xb50 linux/net/tipc/msg.c:186 tipc_link_input+0x224/0x7c0 linux/net/tipc/link.c:1324 tipc_link_rcv+0x76e/0x2d70 linux/net/tipc/link.c:1824 tipc_rcv+0x45f/0x10f0 linux/net/tipc/node.c:2159 tipc_udp_recv+0x73b/0x8f0 linux/net/tipc/udp_media.c:390 udp_queue_rcv_one_skb+0xad2/0x1850 linux/net/ipv4/udp.c:2108 udp_queue_rcv_skb+0x131/0xb00 linux/net/ipv4/udp.c:2186 udp_unicast_rcv_skb+0x165/0x3b0 linux/net/ipv4/udp.c:2346 __udp4_lib_rcv+0x2594/0x3400 linux/net/ipv4/udp.c:2422 ip_protocol_deliver_rcu+0x30c/0x4e0 linux/net/ipv4/ip_input.c:205 ip_local_deliver_finish+0x2e4/0x520 linux/net/ipv4/ip_input.c:233 NF_HOOK linux/./include/linux/netfilter.h:314 NF_HOOK linux/./include/linux/netfilter.h:308 ip_local_deliver+0x18e/0x1f0 linux/net/ipv4/ip_input.c:254 dst_input linux/./include/net/dst.h:461 ip_rcv_finish linux/net/ipv4/ip_input.c:449 NF_HOOK linux/./include/linux/netfilter.h:314 NF_HOOK linux/./include/linux/netfilter.h:308 ip_rcv+0x2c5/0x5d0 linux/net/ipv4/ip_input.c:569 __netif_receive_skb_one_core+0x199/0x1e0 linux/net/core/dev.c:5534 __netif_receive_skb+0x1f/0x1c0 linux/net/core/dev.c:5648 process_backlog+0x101/0x6b0 linux/net/core/dev.c:5976 __napi_poll.constprop.0+0xba/0x550 linux/net/core/dev.c:6576 napi_poll linux/net/core/dev.c:6645 net_rx_action+0x95a/0xe90 linux/net/core/dev.c:6781 __do_softirq+0x21f/0x8e7 linux/kernel/softirq.c:553 do_softirq linux/kernel/softirq.c:454 do_softirq+0xb2/0xf0 linux/kernel/softirq.c:441 </IRQ> <TASK> __local_bh_enable_ip+0x100/0x120 linux/kernel/softirq.c:381 local_bh_enable linux/./include/linux/bottom_half.h:33 rcu_read_unlock_bh linux/./include/linux/rcupdate.h:851 __dev_queue_xmit+0x871/0x3ee0 linux/net/core/dev.c:4378 dev_queue_xmit linux/./include/linux/netdevice.h:3169 neigh_hh_output linux/./include/net/neighbour.h:526 neigh_output linux/./include/net/neighbour.h:540 ip_finish_output2+0x169f/0x2550 linux/net/ipv4/ip_output.c:235 __ip_finish_output linux/net/ipv4/ip_output.c:313 __ip_finish_output+0x49e/0x950 linux/net/ipv4/ip_output.c:295 ip_finish_output+0x31/0x310 linux/net/ipv4/ip_output.c:323 NF_HOOK_COND linux/./include/linux/netfilter.h:303 ip_output+0x13b/0x2a0 linux/net/ipv4/ip_output.c:433 dst_output linux/./include/net/dst.h:451 ip_local_out linux/net/ipv4/ip_output.c:129 ip_send_skb+0x3e5/0x560 linux/net/ipv4/ip_output.c:1492 udp_send_skb+0x73f/0x1530 linux/net/ipv4/udp.c:963 udp_sendmsg+0x1a36/0x2b40 linux/net/ipv4/udp.c:1250 inet_sendmsg+0x105/0x140 linux/net/ipv4/af_inet.c:850 sock_sendmsg_nosec linux/net/socket.c:730 __sock_sendmsg linux/net/socket.c:745 __sys_sendto+0x42c/0x4e0 linux/net/socket.c:2191 __do_sys_sendto linux/net/socket.c:2203 __se_sys_sendto linux/net/socket.c:2199 __x64_sys_sendto+0xe0/0x1c0 linux/net/socket.c:2199 do_syscall_x64 linux/arch/x86/entry/common.c:52 do_syscall_ ---truncated---	8.1	More Details
CVE-2024-36912	In the Linux kernel, the following vulnerability has been resolved: Drivers: hv: vmbus: Track decrypted status in vmbus_gpadl In CoCo VMs it is possible for the untrusted host to cause set_memory_encrypted() or set_memory_decrypted() to fail such that an error is returned and the resulting memory is shared. Callers need to take care to handle these errors to avoid returning decrypted (shared) memory to the page allocator, which could lead to functional or security issues. In order to make sure callers of vmbus_establish_gpadl() and vmbus_teardown_gpadl() don't return decrypted/shared pages to allocators, add a field in struct vmbus_gpadl to keep track of the decryption status of the buffers. This will allow the callers to know if they should free or leak the pages.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29170	Dell PowerScale OneFS versions 8.2.x through 9.8.0.x contain a use of hard coded credentials vulnerability. An adjacent network unauthenticated attacker could potentially exploit this vulnerability, leading to information disclosure of network traffic and denial of service.	8.1	More Details
CVE-2024-36913	In the Linux kernel, the following vulnerability has been resolved: Drivers: hv: vmbus: Leak pages if set_memory_encrypted() fails In CoCo VMs it is possible for the untrusted host to cause set_memory_encrypted() or set_memory_decrypted() to fail such that an error is returned and the resulting memory is shared. Callers need to take care to handle these errors to avoid returning decrypted (shared) memory to the page allocator, which could lead to functional or security issues. VMBus code could free decrypted pages if set_memory_encrypted()/decrypted() fails. Leak the pages if this happens.	8.1	More Details
CVE-2024-36470	In JetBrains TeamCity before 2022.04.7, 2022.10.6, 2023.05.6, 2023.11.5 authentication bypass was possible in specific edge cases	8.1	More Details
CVE-2024-36427	The file-serving function in TARGIT Decision Suite before 24.06.19002 (TARGIT Decision Suite 2024 – June) allows authenticated attackers to read or write to server files via a crafted file request. This can allow code execution via a .xview file.	8.1	More Details
CVE-2024-35433	ZKTeco ZKBio CVSecurity 6.1.1 is vulnerable to Incorrect Access Control. An authenticated user, without the permissions of managing users, can create a new admin user.	8.1	More Details
CVE-2024-37017	asdcplib (aka AS-DCP Lib) 2.13.1 has a heap-based buffer over-read in ASDCP::TimedText::MXFReader::h__Reader::MD_to_TimedText_TDesc in AS_DCP_TimedText.cpp in libasdcp.so.	8.1	More Details
CVE-2024-5565	The Vanna library uses a prompt function to present the user with visualized results, it is possible to alter the prompt using prompt injection and run arbitrary Python code instead of the intended visualization code. Specifically - allowing external input to the library's “ask” method with "visualize" set to True (default behavior) leads to remote code execution.	8.1	More Details
CVE-2024-36120	javascript-deobfuscator removes common JavaScript obfuscation techniques. In affected versions crafted payloads targeting expression simplification can lead to code execution. This issue has been patched in version 1.1.0. Users are advised to update. Users unable to upgrade should disable the expression simplification feature.	8.1	More Details
CVE-2024-5564	A vulnerability was found in libndp. This flaw allows a local malicious user to cause a buffer overflow in NetworkManager, triggered by sending a malformed IPv6 router advertisement packet. This issue occurred as libndp was not correctly validating the route length information.	8.1	More Details
CVE-2024-5138	The snapctl component within snapd allows a confined snap to interact with the snapd daemon to take certain privileged actions on behalf of the snap. It was found that snapctl did not properly parse command-line arguments, allowing an unprivileged user to trigger an authorised action on behalf of the snap that would normally require administrator privileges to perform. This could possibly allow an unprivileged user to perform a denial of service or similar.	8.1	More Details
CVE-2024-36569	Sourcecodester Gas Agency Management System v1.0 is vulnerable to arbitrary code execution via editClientImage.php.	8.1	More Details
CVE-2024-36728	TRENDnet TEW-827DRU devices through 2.06B04 contain a stack-based buffer overflow in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action vlan_setting with a sufficiently long dns1 or dns 2 key.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4611	The AppPresser plugin for WordPress is vulnerable to improper missing encryption exception handling on the 'decrypt_value' and on the 'doCookieAuth' functions in all versions up to, and including, 4.3.2. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they previously used the login via the plugin API. This can only be exploited if the 'openssl' php extension is not loaded on the server.	8.1	More Details
CVE-2024-35430	In ZKTeco ZKBio CVSecurity v6.1.1 an authenticated user can bypass password checks while exporting data from the application.	8.1	More Details
CVE-2024-29828	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an authenticated attacker within the same network to execute arbitrary code.	8.0	More Details
CVE-2024-29829	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an authenticated attacker within the same network to execute arbitrary code.	8.0	More Details
CVE-2024-29830	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an authenticated attacker within the same network to execute arbitrary code.	8.0	More Details
CVE-2024-29846	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an authenticated attacker within the same network to execute arbitrary code.	8.0	More Details
CVE-2024-20874	Improper access control vulnerability in SmartManagerCN prior to SMR Jun-2024 Release 1 allows local attackers to launch privileged activities.	7.9	More Details
CVE-2021-3899	There is a race condition in the 'replaced executable' detection that, with the correct local configuration, allow an attacker to execute arbitrary code as root.	7.8	More Details
CVE-2022-28657	Apport does not disable python crash handler before entering chroot	7.8	More Details
CVE-2023-5751	A local attacker with low privileges can read and modify any users files and cause a DoS in the working directory of the affected products due to exposure of resource to wrong sphere.	7.8	More Details
CVE-2024-37065	Deserialization of untrusted data can occur in versions 0.6 or newer of the skops python library, enabling a maliciously crafted model to run arbitrary code on an end user's system when loaded.	7.8	More Details
CVE-2024-37064	Deseriliazation of untrusted data can occur in versions 3.7.0 or newer of Ydata's ydata-profiling open-source library, enabling a maliciously crafted dataset to run arbitrary code on an end user's system when loaded.	7.8	More Details
CVE-2024-37063	A cross-site scripting (XSS) vulnerability in versions 3.7.0 or newer of Ydata's ydata-profiling open-source library allows for payloads to be run when a maliocusly crafted report is viewed in the browser.	7.8	More Details
CVE-2024-5271	Fuji Electric Monitouch V-SFT is vulnerable to an out-of-bounds write because of a type confusion, which could result in arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37062	Deserialization of untrusted data can occur in versions 3.7.0 or newer of Ydata's ydata-profiling open-source library, enabling a malicously crafted report to run arbitrary code on an end user's system when loaded.	7.8	More Details
CVE-2023-43542	Memory corruption while copying a keyblob`s material when the key material`s size is not accurately checked.	7.8	More Details
CVE-2024-34171	Fuji Electric Monitouch V-SFT is vulnerable to a stack-based buffer overflow, which could allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2024-23667	An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and 6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI.	7.8	More Details
CVE-2024-23670	An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and 6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI.	7.8	More Details
CVE-2024-36955	In the Linux kernel, the following vulnerability has been resolved: ALSA: hda: intel-sdw-acpi: fix usage of device_get_named_child_node() The documentation for device_get_named_child_node() mentions this important point: " The caller is responsible for calling fwnode_handle_put() on the returned fwnode pointer. " Add fwnode_handle_put() to avoid a leaked reference.	7.7	More Details
CVE-2024-36016	In the Linux kernel, the following vulnerability has been resolved: tty: n_gsm: fix possible out-of-bounds in gsm0_receive() Assuming the following: - side A configures the n_gsm in basic option mode - side B sends the header of a basic option mode frame with data length 1 - side A switches to advanced option mode - side B sends 2 data bytes which exceeds gsm->len Reason: gsm->len is not used in advanced option mode. - side A switches to basic option mode - side B keeps sending until gsm0_receive() writes past gsm->buf Reason: Neither gsm->state nor gsm->len have been reset after reconfiguration. Fix this by changing gsm->count to gsm->len comparison from equal to less than. Also add upper limit checks against the constant MAX_MRU in gsm0_receive() and gsm1_receive() to harden against memory corruption of gsm->len and gsm->mru. All other checks remain as we still need to limit the data according to the user configuration and actual payload size.	7.7	More Details
CVE-2024-35140	IBM Security Verify Access Docker 10.0.0 through 10.0.6 could allow a local user to escalate their privileges due to improper certificate validation. IBM X-Force ID: 292416.	7.7	More Details
CVE-2024-35630	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LJ Apps WP TripAdvisor Review Slider allows Blind SQL Injection.This issue affects WP TripAdvisor Review Slider: from n/a through 12.6.	7.6	More Details
CVE-2024-28974	Dell Data Protection Advisor, version(s) 19.9, contain(s) an Inadequate Encryption Strength vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Denial of service.	7.6	More Details
CVE-2024-34363	Envoy is a cloud-native, open source edge and service proxy. Due to how Envoy invoked the nlohmann JSON library, the library could throw an uncaught exception from downstream data if incomplete UTF-8 strings were serialized. The uncaught exception would cause Envoy to crash.	7.5	More Details
CVE-2024-36857	Jan v0.4.12 was discovered to contain an arbitrary file read vulnerability via the /v1/app/readFileSync interface.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34009	Insufficient checks whether ReCAPTCHA was enabled made it possible to bypass the checks on the login page. This did not affect other pages where ReCAPTCHA is utilized.	7.5	More Details
CVE-2024-5000	An unauthenticated remote attacker can use a malicious OPC UA client to send a crafted request to affected CODESYS products which can cause a DoS due to incorrect calculation of buffer size.	7.5	More Details
CVE-2024-36390	MileSight DeviceHub - CWE-20 Improper Input Validation may allow Denial of Service	7.5	More Details
CVE-2024-28996	The SolarWinds Platform was determined to be affected by a SWQL Injection Vulnerability. Attack complexity is high for this vulnerability.	7.5	More Details
CVE-2024-2019	The WP-DB-Table-Editor plugin for WordPress is vulnerable to unauthorized access of data, modification of data, and loss of data due to lack of a default capability requirement on the 'dbte_render' function in all versions up to, and including, 1.8.4. This makes it possible for authenticated attackers, with contributor access and above, to modify database tables that the theme has been configured to use the plugin to edit.	7.5	More Details
CVE-2024-36844	libmodbus v3.1.6 was discovered to contain a use-after-free via the ctx->backend pointer. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted message sent to the unit-test-server.	7.5	More Details
CVE-2024-32871	Pimcore is an Open Source Data & Experience Management Platform. The Pimcore thumbnail generation can be used to flood the server with large files. By changing the file extension or scaling factor of the requested thumbnail, attackers can create files that are much larger in file size than the original. This vulnerability is fixed in 11.2.4.	7.5	More Details
CVE-2024-36843	libmodbus v3.1.6 was discovered to contain a heap overflow via the modbus_mapping_free() function.	7.5	More Details
CVE-2024-23363	Transient DOS while processing an improperly formatted Fine Time Measurement (FTM) management frame.	7.5	More Details
CVE-2024-25095	Insertion of Sensitive Information into Log File vulnerability in Code Parrots Easy Forms for Mailchimp.This issue affects Easy Forms for Mailchimp: from n/a through 6.9.0.	7.5	More Details
CVE-2024-36800	A SQL injection vulnerability in SEMCMS v.4.8, allows a remote attacker to obtain sensitive information via the ID parameter in Download.php.	7.5	More Details
CVE-2024-35492	Cesanta Mongoose commit b316989 was discovered to contain a NULL pointer dereference via the scpy function at src/fmt.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted MQTT packet.	7.5	More Details
CVE-2024-35434	Irontec Sngrep v1.8.1 was discovered to contain a heap buffer overflow via the function rtp_check_packet at /sngrep/src/rtp.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted SIP packet.	7.5	More Details
CVE-2024-35672	Missing Authorization vulnerability in Netgsm.This issue affects Netgsm: from n/a through 2.9.19.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46630	Improper Authentication vulnerability in wpase Admin and Site Enhancements (ASE) allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Admin and Site Enhancements (ASE): from n/a through 5.7.1.	7.5	More Details
CVE-2024-35431	ZKTeco ZKBio CVSecurity 6.1.1 is vulnerable to Directory Traversal via photoBase64. An unauthenticated user can download local files from the server.	7.5	More Details
CVE-2024-4540	A flaw was found in Keycloak in OAuth 2.0 Pushed Authorization Requests (PAR). Client-provided parameters were found to be included in plain text in the KC_RESTART cookie returned by the authorization server's HTTP response to a `request_uri` authorization request, possibly leading to an information disclosure vulnerability.	7.5	More Details
CVE-2024-4520	An improper access control vulnerability exists in the gaizhenbiao/chuanhuchatgpt application, specifically in version 20240410. This vulnerability allows any user on the server to access the chat history of any other user without requiring any form of interaction between the users. Exploitation of this vulnerability could lead to data breaches, including the exposure of sensitive personal details, financial data, or confidential conversations. Additionally, it could facilitate identity theft and manipulation or fraud through the unauthorized access to users' chat histories. This issue is due to insufficient access control mechanisms in the application's handling of chat history data.	7.5	More Details
CVE-2024-36128	Directus is a real-time API and App dashboard for managing SQL database content. Prior to 10.11.2, providing a non-numeric length value to the random string generation utility will create a memory issue breaking the capability to generate random strings platform wide. This creates a denial of service situation where logged in sessions can no longer be refreshed as sessions depend on the capability to generate a random session ID. This vulnerability is fixed in 10.11.2.	7.5	More Details
CVE-2024-36127	apko is an apk-based OCI image builder. apko exposures HTTP basic auth credentials from repository and keyring URLs in log output. This vulnerability is fixed in v0.14.5.	7.5	More Details
CVE-2024-32976	Envoy is a cloud-native, open source edge and service proxy. Envoyproxy with a Brotli filter can get into an endless loop during decompression of Brotli data with extra input.	7.5	More Details
CVE-2023-42005	IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data 3.5, 4.0, 4.5, 4.6, 4.7, and 4.8 could allow a user with access to the Kubernetes pod, to make system calls compromising the security of containers. IBM X-Force ID: 265264.	7.4	More Details
CVE-2024-5185	The EmbedAI application is susceptible to security issues that enable Data Poisoning attacks. This weakness could result in the application becoming compromised, leading to unauthorized entries or data poisoning attacks, which are delivered by a CSRF vulnerability due to the absence of a secure session management implementation and weak CORS policies weakness. An attacker can direct a user to a malicious webpage that exploits a CSRF vulnerability within the EmbedAI application. By leveraging this CSRF vulnerability, the attacker can deceive the user into inadvertently uploading and integrating incorrect data into the application’s language model.	7.3	More Details
CVE-2024-25977	The application does not change the session token when using the login or logout functionality. An attacker can set a session token in the victim's browser (e.g. via XSS) and prompt the victim to log in (e.g. via a redirect to the login page). This results in the victim's account being taken over.	7.3	More Details
CVE-2024-3821	The wpDataTables – WordPress Data Table, Dynamic Tables & Table Charts Plugin plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on several functions in the wdt_ajax_actions.php file in all versions up to, and including, 6.3.2. This makes it possible for unauthenticated attackers to manipulate data tables. Please note this only affects the premium version of the plugin.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5517	A vulnerability was found in itsourcecode Online Blood Bank Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file changepwd.php. The manipulation of the argument useremail 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-266588.	7.3	More Details
CVE-2024-20878	Heap out-of-bound write vulnerability in parsing grid image in libsavscmn.so prior to SMR June-2024 Release 1 allows local attackers to execute arbitrary code.	7.3	More Details
CVE-2024-5519	A vulnerability classified as critical was found in ItsourceCode Learning Management System Project In PHP 1.0. This vulnerability affects unknown code of the file login.php. The manipulation of the argument user_email leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-266590 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2024-20877	Heap out-of-bound write vulnerability in parsing grid image header in libsavscmn.so prior to SMR Jun-2024 Release 1 allows local attackers to execute arbitrary code.	7.3	More Details
CVE-2024-3555	The Social Link Pages: link-in-bio landing pages for your social media profiles plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the import_link_pages() function in all versions up to, and including, 1.6.9. This makes it possible for unauthenticated attackers to inject arbitrary pages and malicious web scripts.	7.2	More Details
CVE-2024-4870	The Frontend Registration – Contact Form 7 plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 5.1 due to insufficient restriction on the '_cf7frr_' post meta. This makes it possible for authenticated attackers, with editor-level access and above, to modify the default user role in the registration form settings.	7.2	More Details
CVE-2024-5207	The POST SMTP – The #1 WordPress SMTP Plugin with Advanced Email Logging and Delivery Failure Notifications plugin for WordPress is vulnerable to time-based SQL Injection via the selected parameter in all versions up to, and including, 2.9.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with administrator access or higher to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.2	More Details
CVE-2024-2793	The Visual Website Collaboration, Feedback & Project Management – Atarim plugin for WordPress is vulnerable to Stored Cross-Site Scripting via comments in all versions up to, and including, 3.30 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-2024-36908	In the Linux kernel, the following vulnerability has been resolved: blk-iocost: do not WARN if iocg was already offlined In iocg_pay_debt(), warn is triggered if 'active_list' is empty, which is intended to confirm iocg is active when it has debt. However, warn can be triggered during a blkcg or disk removal, if iocg_waitq_timer_fn() is run at that time: WARNING: CPU: 0 PID: 2344971 at block/blk-iocost.c:1402 iocg_pay_debt+0x14c/0x190 Call trace: iocg_pay_debt+0x14c/0x190 iocg_kick_waitq+0x438/0x4c0 iocg_waitq_timer_fn+0xd8/0x130 __run_hrtimer+0x144/0x45c __hrtimer_run_queues+0x16c/0x244 hrtimer_interrupt+0x2cc/0x7b0 The warn in this situation is meaningless. Since this iocg is being removed, the state of the 'active_list' is irrelevant, and 'waitq_timer' is canceled after removing 'active_list' in ioc_pd_free(), which ensures iocg is freed after iocg_waitq_timer_fn() returns. Therefore, add the check if iocg was already offlined to avoid warn when removing a blkcg or disk.	7.1	More Details
CVE-2024-35668	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Brevo Newsletter, SMTP, Email marketing and Subscribe forms by Sendinblue allows Reflected XSS.This issue affects Newsletter, SMTP, Email marketing and Subscribe forms by Sendinblue: from n/a through 3.1.77.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29004	The SolarWinds Platform was determined to be affected by a stored cross-site scripting vulnerability affecting the web console. A high-privileged user and user interaction is required to exploit this vulnerability.	7.1	More Details
CVE-2024-35428	ZKTeco ZKBio CVSecurity 6.1.1 is vulnerable to Directory Traversal via BaseMediaFile. An authenticated user can delete local files from the server which can lead to DoS.	7.1	More Details
CVE-2024-35631	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Foliovision FV Flowplayer Video Player allows Reflected XSS.This issue affects FV Flowplayer Video Player: from n/a through 7.5.45.7212.	7.1	More Details
CVE-2024-35652	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Saso Nikolov Event Tickets with Ticket Scanner allows Reflected XSS.This issue affects Event Tickets with Ticket Scanner: from n/a through 2.3.1.	7.1	More Details
CVE-2024-4958	The User Registration – Custom Registration Form, Login Form, and User Profile WordPress Plugin plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'import_form_action' function in versions up to, and including, 3.2.0.1. This makes it possible for authenticated attackers, with contributor-level permissions and above, to import a registration form with a default user role of administrator. If an administrator approves or publishes a post or page with the shortcode to the imported form, any user can register as an administrator.	7.1	More Details
CVE-2024-28736	An issue in Debezium Community debezium-ui v.2.5 allows a local attacker to execute arbitrary code via the refresh page function.	7.1	More Details
CVE-2024-34794	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Tainacan.Org Tainacan allows Reflected XSS.This issue affects Tainacan: from n/a through 0.21.3.	7.1	More Details
CVE-2024-36030	In the Linux kernel, the following vulnerability has been resolved: octeontx2-af: fix the double free in rvu_npc_freemem() Clang static checker(scan-build) warning：drivers/net/ethernet/marvell/octeontx2/af/rvu_npc.c:line 2184, column 2 Attempt to free released memory. npc_mcam_rsrcs_deinit() has released 'mcam->counters.bmap'. Deleted this redundant kfree() to fix this double free problem.	7.1	More Details
CVE-2022-28655	is_closing_session() allows users to create arbitrary tcp dbus connections	7.1	More Details
CVE-2024-35664	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPvivid Team WPvivid Backup for MainWP allows Reflected XSS.This issue affects WPvivid Backup for MainWP: from n/a through 0.9.32.	7.1	More Details
CVE-2024-36365	In JetBrains TeamCity before 2022.04.7, 2022.10.6, 2023.05.6, 2023.11.5, 2024.03.2 a third-party agent could impersonate a cloud agent	6.8	More Details
CVE-2023-43543	Memory corruption in Audio during a playback or a recording due to race condition between allocation and deallocation of graph object.	6.7	More Details
CVE-2023-52162	Mercusys MW325R EU V3 (Firmware MW325R(EU)_V3_1.11.0 Build 221019) is vulnerable to a stack-based buffer overflow, which could allow an attacker to execute arbitrary code. Exploiting the vulnerability requires authentication.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43544	Memory corruption when IPC callback handle is used after it has been released during register callback by another thread.	6.7	More Details
CVE-2023-43545	Memory corruption when more scan frequency list or channels are sent from the user space.	6.7	More Details
CVE-2024-29975	** UNSUPPORTED WHEN ASSIGNED ** The improper privilege management vulnerability in the SUID executable binary in Zyxel NAS326 firmware versions before V5.21(AAZF.17)C0 and NAS542 firmware versions before V5.21(ABAG.14)C0 could allow an authenticated local attacker with administrator privileges to execute some system commands as the “root” user on a vulnerable device.	6.7	More Details
CVE-2024-20074	In dmc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08668110; Issue ID: MSV-1333.	6.6	More Details
CVE-2024-20073	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00367704; Issue ID: MSV-1411.	6.6	More Details
CVE-2024-20072	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00364732; Issue ID: MSV-1332.	6.6	More Details
CVE-2023-51511	Improper Authentication vulnerability in Pluggabl LLC Booster Elite for WooCommerce allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Booster Elite for WooCommerce: from n/a before 7.1.3.	6.5	More Details
CVE-2024-35429	ZKTeco ZKBio CVSecurity 6.1.1 is vulnerable to Directory Traversal via eventRecord.	6.5	More Details
CVE-2023-48747	Improper Authentication vulnerability in Pluggabl LLC Booster for WooCommerce allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Booster for WooCommerce: from n/a through 7.1.2.	6.5	More Details
CVE-2024-34002	In a shared hosting environment that has been misconfigured to allow access to other users' content, a Moodle user with both access to restore feedback modules and direct access to the web server outside of the Moodle webroot could execute a local file include.	6.5	More Details
CVE-2024-25975	The application implements an up- and downvote function which alters a value within a JSON file. The POST parameters are not filtered properly and therefore an arbitrary file can be overwritten. The file can be controlled by an authenticated attacker, the content cannot be controlled. It is possible to overwrite all files for which the webserver has write access. It is required to supply a relative path (path traversal).	6.5	More Details
CVE-2024-36362	In JetBrains TeamCity before 2022.04.7, 2022.10.6, 2023.05.6, 2023.11.5, 2024.03.2 path traversal allowing to read files from server was possible	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35189	Fides is an open-source privacy engineering platform. The Fides webserver has a number of endpoints that retrieve `ConnectionConfiguration` records and their associated `secrets` which _can_ contain sensitive data (e.g. passwords, private keys, etc.). These `secrets` are stored encrypted at rest (in the application database), and the associated endpoints are not meant to expose that sensitive data in plaintext to API clients, as it could be compromising. Fides's developers have available to them a Pydantic field-attribute (`sensitive`) that they can annotate as `True` to indicate that a given secret field should not be exposed via the API. The application has an internal function that uses `sensitive` annotations to mask the sensitive fields with a `"**********"` placeholder value. This vulnerability is due to a bug in that function, which prevented `sensitive` API model fields that were _nested_ below the root-level of a `secrets` object from being masked appropriately. Only the `BigQuery` connection configuration secrets meets these criteria: the secrets schema has a nested sensitive `keyfile_creds.private_key` property that is exposed in plaintext via the APIs. Connection types other than `BigQuery` with sensitive fields at the root-level that are not nested are properly masked with the placeholder and are not affected by this vulnerability. This vulnerability has been patched in Fides version 2.37.0. Users are advised to upgrade to this version or later to secure their systems against this threat. Users are also advised to rotate any Google Cloud secrets used for BigQuery integrations in their Fides deployments. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2023-49852	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Vsourz Digital Responsive Slick Slider WordPress allows Code Injection.This issue affects Responsive Slick Slider WordPress: from n/a through 1.4.	6.5	More Details
CVE-2024-36364	In JetBrains TeamCity before 2022.04.7, 2022.10.6, 2023.05.6, 2023.11.5 improper access control in Pull Requests and Commit status publisher build features was possible	6.5	More Details
CVE-2024-36377	In JetBrains TeamCity before 2024.03.2 certain TeamCity API endpoints did not check user permissions	6.5	More Details
CVE-2024-36376	In JetBrains TeamCity before 2024.03.2 users could perform actions that should not be available to them based on their permissions	6.5	More Details
CVE-2021-44534	Insufficient user input filtering leads to arbitrary file read by non-authenticated attacker, which results in sensitive information disclosure.	6.5	More Details
CVE-2024-5463	A vulnerability regarding buffer copy without checking the size of input ('Classic Buffer Overflow') has been found in the login component. This allows remote attackers to conduct denial-of-service attacks via unspecified vectors. This attack only affects the login service which will automatically restart. The following models with Synology Camera Firmware versions before 1.1.1-0383 may be affected: BC500 and TC500.	6.5	More Details
CVE-2024-33541	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in BetterAddons Better Elementor Addons allows PHP Local File Inclusion.This issue affects Better Elementor Addons: from n/a through 1.4.1.	6.5	More Details
CVE-2024-34005	In a shared hosting environment that has been misconfigured to allow access to other users' content, a Moodle user with both access to restore database activity modules and direct access to the web server outside of the Moodle webroot could execute a local file include.	6.5	More Details
CVE-2024-34795	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Tainacan.Org Tainacan allows Stored XSS.This issue affects Tainacan: from n/a through 0.21.3.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40673	: Improper Control of Interaction Frequency vulnerability in cartpauj Cartpauj Register Captcha allows Functionality Misuse.This issue affects Cartpauj Register Captcha: from n/a through 1.0.02.	6.5	More Details
CVE-2023-43537	Information disclosure while handling T2LM Action Frame in WLAN Host.	6.5	More Details
CVE-2024-35651	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Spiffy Plugins WP Flow Plus allows Stored XSS.This issue affects WP Flow Plus: from n/a through 5.2.2.	6.5	More Details
CVE-2024-35653	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in visualcomposer.Com Visual Composer Website Builder allows Stored XSS.This issue affects Visual Composer Website Builder: from n/a through 45.8.0.	6.5	More Details
CVE-2024-34789	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Hait Post Grid Elementor Addon allows Stored XSS.This issue affects Post Grid Elementor Addon: from n/a through 2.0.16.	6.5	More Details
CVE-2024-34791	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in wpbean WPB Elementor Addons allows Stored XSS.This issue affects WPB Elementor Addons: from n/a through 1.0.9.	6.5	More Details
CVE-2024-34759	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in VideoWhisper Picture Gallery allows Stored XSS.This issue affects Picture Gallery: from n/a through 1.5.11.	6.5	More Details
CVE-2024-34801	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Mervin Praison Praison SEO WordPress allows Stored XSS.This issue affects Praison SEO WordPress: from n/a through 4.0.15.	6.5	More Details
CVE-2024-35358	A vulnerability has been discovered in Diño Physics School Assistant version 2.3. The vulnerability impacts an unidentified code within the file /classes/Master.php?f=view_category. Manipulating the argument id can result in SQL injection.	6.5	More Details
CVE-2024-34764	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPDeveloper Essential Addons for Elementor allows Stored XSS.This issue affects Essential Addons for Elementor: from n/a through 5.9.15.	6.5	More Details
CVE-2024-34766	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Automattic ChaosTheory allows Stored XSS.This issue affects ChaosTheory: from n/a through 1.3.	6.5	More Details
CVE-2024-34767	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in HasThemes ShopLentor allows Stored XSS.This issue affects ShopLentor: from n/a through 2.8.7.	6.5	More Details
CVE-2024-34769	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in cyclonetheme Elegant Blocks allows Stored XSS.This issue affects Elegant Blocks: from n/a through 1.7.	6.5	More Details
CVE-2024-34770	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Popup Maker Popup Maker WP allows Stored XSS.This issue affects Popup Maker WP: from n/a through 1.2.8.	6.5	More Details
CVE-2023-38520	External Control of Assumed-Immutable Web Parameter vulnerability in PINPOINT.WORLD Pinpoint Booking System allows Functionality Misuse.This issue affects Pinpoint Booking System: from n/a through 2.9.9.3.4.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36123	Citizen is a MediaWiki skin that makes extensions part of the cohesive experience. The page `MediaWiki:Tagline` has its contents used unescaped, so custom HTML (including Javascript) can be injected by someone with the ability to edit the MediaWiki namespace (typically those with the `editinterface` permission, or sysops). This vulnerability is fixed in 2.16.0.	6.5	More Details
CVE-2023-51219	A deep link validation issue in KakaoTalk 10.4.3 allowed a remote adversary to direct users to run any attacker-controlled JavaScript within a WebView. The impact was further escalated by triggering another WebView that leaked its access token in a HTTP request header. Ultimately, this access token could be used to take over another user's account and read her/his chat messages.	6.5	More Details
CVE-2024-29976	** UNSUPPORTED WHEN ASSIGNED ** The improper privilege management vulnerability in the command “show_allsessions” in Zyxel NAS326 firmware versions before V5.21(AAZF.17)C0 and NAS542 firmware versions before V5.21(ABAG.14)C0 could allow an authenticated attacker to obtain a logged-in administrator’s session information containing cookies on an affected device.	6.5	More Details
CVE-2024-35649	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Pdfcrowd Save as PDF plugin by Pdfcrowd allows Stored XSS.This issue affects Save as PDF plugin by Pdfcrowd: from n/a through 3.2.3.	6.5	More Details
CVE-2024-20069	In modem, there is a possible selection of less-secure algorithm during the VoWiFi IKE due to a missing DH downgrade check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01286330; Issue ID: MSV-1430.	6.5	More Details
CVE-2024-31493	An improper removal of sensitive information before storage or transfer vulnerability [CWE-212] in FortiSOAR version 7.3.0, version 7.2.2 and below, version 7.0.3 and below may allow an authenticated low privileged user to read Connector passwords in plain-text via HTTP responses.	6.5	More Details
CVE-2024-35782	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Codeless Cowidgets – Elementor Addons allows Stored XSS.This issue affects Cowidgets – Elementor Addons: from n/a through 1.1.1.	6.5	More Details
CVE-2024-35666	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themesflat Themesflat Addons For Elementor allows Stored XSS.This issue affects Themesflat Addons For Elementor: from n/a through 2.1.2.	6.5	More Details
CVE-2024-32760	When NGINX Plus or NGINX OSS are configured to use the HTTP/3 QUIC module, undisclosed HTTP/3 encoder instructions can cause NGINX worker processes to terminate or cause or other potential impact.	6.5	More Details
CVE-2024-4218	The AffiEasy plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.7. This is due to plugin improperly releasing the tagged and patched version of the plugin - the vulnerable version is used as the core files, while the patched version was included in a 'trunk' folder. This makes it possible for unauthenticated attackers to perform a variety of actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.5	More Details
CVE-2023-42427	Cross-site scripting vulnerability exists in UNIVERSAL PASSPORT RX versions 1.0.0 to 1.0.7, which may allow a remote authenticated attacker to execute an arbitrary script on the web browser of the user who is using the product.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36916	In the Linux kernel, the following vulnerability has been resolved: blk-iocost: avoid out of bounds shift UBSAN catches undefined behavior in blk-iocost, where sometimes iocg->delay is shifted right by a number that is too large, resulting in undefined behavior on some architectures. [186.556576] ----------[cut here]----------- UBSAN: shift-out-of-bounds in block/blk-iocost.c:1366:23 shift exponent 64 is too large for 64-bit type 'u64' (aka 'unsigned long long') CPU: 16 PID: 0 Comm: swapper/16 Tainted: G S E N 6.9.0-0_fbk700_debug_rc2_kbuilder_0_gc85af715cac0 #1 Hardware name: Quanta Twin Lakes MP/Twin Lakes Passive MP, BIOS F09_3A23 12/08/2020 Call Trace: <IRQ> dump_stack_lvl+0x8f/0xe0 __ubsan_handle_shift_out_of_bounds+0x22c/0x280 iocg_kick_delay+0x30b/0x310 ioc_timer_fn+0x2fb/0x1f80 __run_timer_base+0x1b6/0x250 ... Avoid that undefined behavior by simply taking the "delay = 0" branch if the shift is too large. I am not sure what the symptoms of an undefined value delay will be, but I suspect it could be more than a little annoying to debug.	6.5	More Details
CVE-2024-35654	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CyberChimps Responsive allows Stored XSS.This issue affects Responsive: from n/a through 5.0.3.	6.5	More Details
CVE-2024-34384	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in SinaExtra Sina Extension for Elementor allows PHP Local File Inclusion.This issue affects Sina Extension for Elementor: from n/a through 3.5.1.	6.5	More Details
CVE-2024-3888	The tagDiv Composer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's button shortcode in all versions up to, and including, 4.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. NOTE: The vulnerable code in this plugin is specifically tied to the tagDiv Newspaper theme. If another theme is installed (e.g., NewsMag), this code may not be present.	6.4	More Details
CVE-2024-3565	The Content Blocks (Custom Post Widget) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'content_block' shortcode in all versions up to, and including, 3.3.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4160	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wpdm-all-packages' shortcode in all versions up to, and including, 3.2.90 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-6382	The Master Slider – Responsive Touch Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ms_slide' shortcode in all versions up to, and including, 3.9.9 due to insufficient input sanitization and output escaping on user supplied 'css_class' attribute. 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-2024-5427	The WPCafe – Online Food Ordering, Restaurant Menu, Delivery, and Reservations for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Reservation Form shortcode in all versions up to, and including, 2.2.24 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3230	The Download Attachments plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'download-attachments' shortcode in all versions up to, and including, 1.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-20880	Stack-based buffer overflow vulnerability in bootloader prior to SMR Jun-2024 Release 1 allows physical attackers to overwrite memory.	6.4	More Details
CVE-2024-4376	The Premium Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Fancy Text widget in all versions up to, and including, 4.10.31 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. While 4.10.32 is patched, it is recommended to update to 4.10.33 because 4.10.32 caused a fatal error.	6.4	More Details
CVE-2024-5347	The Happy Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'arrow' attribute within the plugin's Post Navigation widget in all versions up to, and including, 3.10.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4273	The Essential Real Estate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ere_property_map' shortcode in all versions up to, and including, 4.4.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4697	The Cowidgets – Elementor Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘heading_tag’ parameter in all versions up to, and including, 1.1.1 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-2024-5418	The DethemeKit For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'slitems' attribute within the plugin's De Product Tab & Slide widget in all versions up to, and including, 2.1.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5041	The Happy Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘ha-ia-content-button’ parameter in all versions up to, and including, 3.10.9 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-2024-5485	The SureTriggers – Connect All Your Plugins, Apps, Tools & Automate Everything! plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Trigger Link shortcode in all versions up to, and including, 1.0.47 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-31908	IBM Planning Analytics Local 2.0 and 2.1 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 289890.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-7073	The Auto Featured Image (Auto Post Thumbnail) plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 4.0.0 via the upload_to_library AJAX action. This makes it possible for authenticated attackers, with author-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	6.4	More Details
CVE-2024-20881	Improper input validation vulnerability in chnactiv TA prior to SMR Jun-2024 Release 1 allows local privileged attackers lead to potential arbitrary code execution.	6.4	More Details
CVE-2024-5501	The Supreme Modules Lite – Divi Theme, Extra Theme and Divi Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'button_one_id' parameter in all versions up to, and including, 2.5.51 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-2024-2506	The Popup Builder – Create highly converting, mobile friendly marketing popups. plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the custom JS functionality in all versions up to, and including, 4.2.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4711	The WordPress Infinite Scroll – Ajax Load More plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ajax_load_more shortcode in versions up to, and including, 7.1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2933	The Page Builder Gutenberg Blocks – CoBlocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Social Profiles widget in all versions up to, and including, 3.1.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2295	The Contact Form Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's [xyz-cfm-form] shortcode in all versions up to, and including, 1.6.1 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-2024-4581	The Slider Revolution plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Add Layer widget in all versions up to, and including, 6.7.11 due to insufficient input sanitization and output escaping on the user supplied 'class', 'id', and 'title' attributes. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. NOTE: Successful exploitation of this vulnerability requires an Administrator to give Slider Creation privileges to Author-level users.	6.4	More Details
CVE-2024-5039	The HUSKY – Products Filter Professional 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, 1.3.5.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4087	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Back to Top widget in all versions up to, and including, 1.3.975 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4637	The Slider Revolution plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 6.7.10 due to insufficient input sanitization and output escaping on the user supplied Elementor 'wrapperid' and 'zindex' display attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5086	The Essential Addons for Elementor PRO – Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Team Member Carousel widget in all Pro versions up to, and including, 5.8.14 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4342	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's image hotspot, image accordion, off canvas, woogrid, and product mini cart widgets in all versions up to, and including, 1.3.975 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4422	The Comparison Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the slider title parameter in all versions up to, and including, 1.0.5 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-2024-2253	The Testimonial Carousel For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via URL values the plugin's carousel widgets in all versions up to, and including, 10.2.1 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-2024-3726	The Login Logout Register Menu plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'llrmloginlogout' shortcode in all versions up to, and including, 2.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5327	The PowerPack Addons for Elementor (Free Widgets, Extensions and Templates) plugin for WordPress is vulnerable to DOM-Based Stored Cross-Site Scripting via the ‘pp_animated_gradient_bg_color’ parameter in all versions up to, and including, 2.7.19 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-2024-5341	The The Plus Addons for Elementor Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'size' attribute of the Heading Title widget in all versions up to, and including, 5.5.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5073	The Essential Addons for Elementor – Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Twitter Feed component in all versions up to, and including, 5.9.21 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-2024-4356	The List categories plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'categories' shortcode in all versions up to, and including, 0.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-28999	The SolarWinds Platform was determined to be affected by a Race Condition Vulnerability affecting the web console.	6.4	More Details
CVE-2024-5521	Two Cross-Site Scripting vulnerabilities have been discovered in Alkacon's OpenCMS affecting version 16, which could allow a user having the roles of gallery editor or VFS resource manager will have the permission to upload images in the .svg format containing JavaScript code. The code will be executed the moment another user accesses the image.	6.4	More Details
CVE-2024-3063	The WPB Elementor Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the output of 'tags' added to widgets in all versions up to, and including, 1.0.9 due to insufficient input sanitization and output escaping on user supplied tag attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-3583	The Simple Like Page Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 1.5.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5520	Two Cross-Site Scripting vulnerabilities have been discovered in Alkacon's OpenCMS affecting version 16, which could allow a user with sufficient privileges to create and modify web pages through the admin panel, can execute malicious JavaScript code, after inserting code in the “title” field.	6.4	More Details
CVE-2024-4668	The Gum Elementor Addon plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Price Table and Post Slider widgets in all versions up to, and including, 1.3.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5223	The Post Grid Gutenberg Blocks and WordPress Blog Plugin – PostX plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's file uploading feature in all versions up to, and including, 4.1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5590	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3. It has been declared as critical. This vulnerability affects unknown code of the file /protocol/iscuser/uploadiscuser.php of the component JSON Content Handler. The manipulation of the argument messagecontent leads to sql injection. 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-266848. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5635	A vulnerability was found in itsourcecode Bakery Online Ordering System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file index.php. The manipulation of the argument txtsearch 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-267091.	6.3	More Details
CVE-2024-5516	A vulnerability was found in itsourcecode Online Blood Bank Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file massage.php. The manipulation of the argument bid 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-266587.	6.3	More Details
CVE-2024-5518	A vulnerability classified as critical has been found in itsourcecode Online Discussion Forum 1.0. This affects an unknown part of the file change_profile_picture.php. The manipulation of the argument image leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-266589 was assigned to this vulnerability.	6.3	More Details
CVE-2024-35356	A vulnerability has been discovered in Diño Physics School Assistant version 2.3. The vulnerability impacts an unidentified code within the file /classes/Master.php?f=save_item. Manipulating the argument id can result in SQL injection.	6.3	More Details
CVE-2024-5588	A vulnerability was found in itsourcecode Learning Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file processscore.php. The manipulation of the argument LessonID 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-266839.	6.3	More Details
CVE-2024-5515	A vulnerability was found in SourceCodester Stock Management System 1.0. It has been classified as critical. Affected is an unknown function of the file createBrand.php. The manipulation of the argument brandName 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-266586 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-5589	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 /admin/config_MT.php?action=delete. The manipulation of the argument Mid 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 associated identifier of this vulnerability is VDB-266847. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-27313	Zoho ManageEngine PAM360 is vulnerable to Stored XSS vulnerability. This vulnerability is applicable only in the version 6610.	6.3	More Details
CVE-2024-20886	Arbitrary directory creation in Samsung Live Wallpaper PC prior to version 3.3.8.0 allows attacker to create arbitrary directory.	6.2	More Details
CVE-2024-20887	Arbitrary directory creation in GalaxyBudsManager PC prior to version 2.1.240315.51 allows attacker to create arbitrary directory.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36888	In the Linux kernel, the following vulnerability has been resolved: workqueue: Fix selection of wake_cpu in kick_pool() With cpu_possible_mask=0-63 and cpu_online_mask=0-7 the following kernel oops was observed: smp: Bringing up secondary CPUs ... smp: Brought up 1 node, 8 CPUs Unable to handle kernel pointer dereference in virtual kernel address space Failing address: 0000000000000000 TEID: 0000000000000803 [..] Call Trace: arch_vcpu_is_preempted+0x12/0x80 select_idle_sibling+0x42/0x560 select_task_rq_fair+0x29a/0x3b0 try_to_wake_up+0x38e/0x6e0 kick_pool+0xa4/0x198 __queue_work.part.0+0x2bc/0x3a8 call_timer_fn+0x36/0x160 __run_timers+0x1e2/0x328 __run_timer_base+0x5a/0x88 run_timer_softirq+0x40/0x78 __do_softirq+0x118/0x388 irq_exit_rcu+0xc0/0xd8 do_ext_irq+0xae/0x168 ext_int_handler+0xbe/0xf0 psw_idle_exit+0x0/0xc default_idle_call+0x3c/0x110 do_idle+0xd4/0x158 cpu_startup_entry+0x40/0x48 rest_init+0xc6/0xc8 start_kernel+0x3c4/0x5e0 startup_continue+0x3c/0x50 The crash is caused by calling arch_vcpu_is_preempted() for an offline CPU. To avoid this, select the cpu with cpumask_any_and_distribute() to mask __pod_cpumask with cpu_online_mask. In case no cpu is left in the pool, skip the assignment. tj: This doesn't fully fix the bug as CPUs can still go down between picking the target CPU and the wake call. Fixing that likely requires adding cpu_online() test to either the sched or s390 arch code. However, regardless of how that is fixed, workqueue shouldn't be picking a CPU which isn't online as that would result in unpredictable and worse behavior.	6.2	More Details
CVE-2024-20884	Incorrect use of privileged API vulnerability in getSemBatteryUsageStats in BatteryStatsService prior to SMR Jun-2024 Release 1 allows local attackers to use privileged API.	6.2	More Details
CVE-2024-36910	In the Linux kernel, the following vulnerability has been resolved: uio_hv_generic: Don't free decrypted memory In CoCo VMs it is possible for the untrusted host to cause set_memory_encrypted() or set_memory_decrypted() to fail such that an error is returned and the resulting memory is shared. Callers need to take care to handle these errors to avoid returning decrypted (shared) memory to the page allocator, which could lead to functional or security issues. The VMBus device UIO driver could free decrypted/shared pages if set_memory_decrypted() fails. Check the decrypted field in the gpadl to decide whether to free the memory.	6.2	More Details
CVE-2024-33996	Incorrect validation of allowed event types in a calendar web service made it possible for some users to create events with types/audiences they did not have permission to publish to.	6.2	More Details
CVE-2024-20883	Incorrect use of privileged API vulnerability in registerBatteryStatsCallback in BatteryStatsService prior to SMR Jun-2024 Release 1 allows local attackers to use privileged API.	6.2	More Details
CVE-2024-21478	transient DOS when setting up a fence callback to free a KGSL memory entry object during DMA.	6.2	More Details
CVE-2024-36962	In the Linux kernel, the following vulnerability has been resolved: net: ks8851: Queue RX packets in IRQ handler instead of disabling BHs Currently the driver uses local_bh_disable()/local_bh_enable() in its IRQ handler to avoid triggering net_rx_action() softirq on exit from netif_rx(). The net_rx_action() could trigger this driver .start_xmit callback, which is protected by the same lock as the IRQ handler, so calling the .start_xmit from netif_rx() from the IRQ handler critical section protected by the lock could lead to an attempt to claim the already claimed lock, and a hang. The local_bh_disable()/local_bh_enable() approach works only in case the IRQ handler is protected by a spinlock, but does not work if the IRQ handler is protected by mutex, i.e. this works for KS8851 with Parallel bus interface, but not for KS8851 with SPI bus interface. Remove the BH manipulation and instead of calling netif_rx() inside the IRQ handler code protected by the lock, queue all the received SKBs in the IRQ handler into a queue first, and once the IRQ handler exits the critical section protected by the lock, dequeue all the queued SKBs and push them all into netif_rx(). At this point, it is safe to trigger the net_rx_action() softirq, since the netif_rx() call is outside of the lock that protects the IRQ handler.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37031	The Active Admin (aka activeadmin) framework before 3.2.2 for Ruby on Rails allows stored XSS in certain situations where users can create entities (to be later edited in forms) with arbitrary names, aka a "dynamic form legends" issue. 4.0.0.beta7 is also a fixed version.	6.1	More Details
CVE-2024-4057	The Gutenberg Blocks with AI by Kadence WP WordPress plugin before 3.2.37 does not validate and escape some of its block attributes before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	6.1	More Details
CVE-2024-23664	A URL redirection to untrusted site ('open redirect') in Fortinet FortiAuthenticator version 6.6.0, version 6.5.3 and below, version 6.4.9 and below may allow an attacker to to redirect users to an arbitrary website via a crafted URL.	6.1	More Details
CVE-2024-36392	MileSight DeviceHub - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details
CVE-2022-25038	wanEditor v4.7.11 was discovered to contain a cross-site scripting (XSS) vulnerability via the video upload function.	6.1	More Details
CVE-2024-35283	A vulnerability in the Ignite component of Mitel MiContact Center Business through 10.0.0.4 could allow an unauthenticated attacker to conduct a stored cross-site scripting (XSS) attack due to insufficient input validation.	6.1	More Details
CVE-2024-35432	ZKTeco ZKBio CVSecurity 6.1.1 is vulnerable to Cross Site Scripting (XSS) via an Audio File. An authenticated user can injection malicious JavaScript code to trigger a Cross Site Scripting.	6.1	More Details
CVE-2024-35352	A vulnerability has been discovered in Diño Physics School Assistant version 2.3. This vulnerability impacts unidentified code within the file /classes/Users.php?f=save. Manipulating the parameter middlename results in cross-site scripting.	6.1	More Details
CVE-2024-32464	Action Text brings rich text content and editing to Rails. Instances of ActionText::Attachable::ContentAttachment included within a rich_text_area tag could potentially contain unsanitized HTML. This vulnerability is fixed in 7.1.3.4 and 7.2.0.beta2.	6.1	More Details
CVE-2024-20876	Improper input validation in libsheifdecadapter.so prior to SMR Jun-2024 Release 1 allows local attackers to lead to memory corruption.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36674	LyLme_spage v1.9.5 is vulnerable to Cross Site Scripting (XSS) via admin/link.php.	6.1	More Details
CVE-2024-33997	Additional sanitizing was required when opening the equation editor to prevent a stored XSS risk when editing another user's equation.	6.1	More Details
CVE-2024-1298	EDK2 contains a vulnerability when S3 sleep is activated where an Attacker may cause a Division-By-Zero due to a UNIT32 overflow via local access. A successful exploit of this vulnerability may lead to a loss of Availability.	6.0	More Details
CVE-2023-51436	Cross-site scripting vulnerability exists in UNIVERSAL PASSPORT RX versions 1.0.0 to 1.0.8, which may allow a remote authenticated attacker with an administrative privilege to execute an arbitrary script on the web browser of the user who is using the product.	5.9	More Details
CVE-2024-23665	Multiple improper authorization vulnerabilities [CWE-285] in FortiWeb version 7.4.2 and below, version 7.2.7 and below, version 7.0.10 and below, version 6.4.3 and below, version 6.3.23 and below may allow an authenticated attacker to perform unauthorized ADOM operations via crafted requests.	5.9	More Details
CVE-2024-35639	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Webliberty Simple Spoiler allows Stored XSS.This issue affects Simple Spoiler: from n/a through 1.2.	5.9	More Details
CVE-2024-35655	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Brave Brave Popup Builder allows Stored XSS.This issue affects Brave Popup Builder: from n/a through 0.6.9.	5.9	More Details
CVE-2024-35646	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Smartarget Smartarget Message Bar allows Stored XSS.This issue affects Smartarget Message Bar: from n/a through 1.3.	5.9	More Details
CVE-2024-35645	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in vinoth06 Random Banner allows Stored XSS.This issue affects Random Banner: from n/a through 4.2.8.	5.9	More Details
CVE-2024-34003	In a shared hosting environment that has been misconfigured to allow access to other users' content, a Moodle user with both access to restore workshop modules and direct access to the web server outside of the Moodle webroot could execute a local file include.	5.9	More Details
CVE-2024-34385	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in YITH YITH WooCommerce Wishlist allows Stored XSS.This issue affects YITH WooCommerce Wishlist: from n/a through 3.32.0.	5.9	More Details
CVE-2024-36801	A SQL injection vulnerability in SEMCMS v.4.8, allows a remote attacker to obtain sensitive information via the lgid parameter in Download.php.	5.9	More Details
CVE-2024-34797	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Benoit Mercusot Simple Popup Manager allows Stored XSS.This issue affects Simple Popup Manager: from n/a through 1.3.5.	5.9	More Details
CVE-2024-34796	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in AccessAlly PopupAlly allows Stored XSS.This issue affects PopupAlly: from n/a through 2.1.1.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29152	An issue was discovered in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, Exynos 990, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 2400, Exynos Modem 5123, and Exynos Modem 5300. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information.	5.9	More Details
CVE-2024-34790	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Hans van Eijsden,niwreg ImageMagick Sharpen Resized Images allows Stored XSS.This issue affects ImageMagick Sharpen Resized Images: from n/a through 1.1.7.	5.9	More Details
CVE-2024-35647	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Global Notification Bar allows Stored XSS.This issue affects Global Notification Bar: from n/a through 1.0.1.	5.9	More Details
CVE-2024-34362	Envoy is a cloud-native, open source edge and service proxy. There is a use-after-free in `HttpConnectionManager` (HCM) with `EnvoyQuicServerStream` that can crash Envoy. An attacker can exploit this vulnerability by sending a request without `FIN`, then a `RESET_STREAM` frame, and then after receiving the response, closing the connection.	5.9	More Details
CVE-2024-36121	netty-incubator-codec-ohttp is the OHTTP implementation for netty. BoringSSLAEADContext keeps track of how many OHTTP responses have been sent and uses this sequence number to calculate the appropriate nonce to use with the encryption algorithm. Unfortunately, two separate errors combine which would allow an attacker to cause the sequence number to overflow and thus the nonce to repeat.	5.9	More Details
CVE-2024-35641	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in GregRoss Just Writing Statistics allows Stored XSS.This issue affects Just Writing Statistics: from n/a through 4.5.	5.9	More Details
CVE-2024-35640	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Tomas Cordero Safety Exit allows Stored XSS.This issue affects Safety Exit: from n/a through 1.7.0.	5.9	More Details
CVE-2024-23847	Incorrect default permissions issue exists in Unifier and Unifier Cast Version.5.0 or later, and the patch "20240527" not applied. If this vulnerability is exploited, arbitrary code may be executed with LocalSystem privilege. As a result, a malicious program may be installed, data may be modified or deleted.	5.9	More Details
CVE-2024-36378	In JetBrains TeamCity before 2024.03.2 server was susceptible to DoS attacks with incorrect auth tokens	5.9	More Details
CVE-2024-23326	Envoy is a cloud-native, open source edge and service proxy. A theoretical request smuggling vulnerability exists through Envoy if a server can be tricked into adding an upgrade header into a response. Per RFC https://www.rfc-editor.org/rfc/rfc7230#section-6.7 a server sends 101 when switching protocols. Envoy incorrectly accepts a 200 response from a server when requesting a protocol upgrade, but 200 does not indicate protocol switch. This opens up the possibility of request smuggling through Envoy if the server can be tricked into adding the upgrade header to the response.	5.9	More Details
CVE-2024-35642	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Bryan Hadaway Site Favicon allows Stored XSS.This issue affects Site Favicon: from n/a through 0.2.	5.9	More Details
CVE-2024-35643	Cross Site Scripting (XSS) vulnerability in Xabier Miranda WP Back Button allows Stored XSS.This issue affects WP Back Button: from n/a through 1.1.3.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20068	In modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is no needed for exploitation. Patch ID: MOLY01270721; Issue ID: MSV-1479.	5.9	More Details
CVE-2024-32975	Envoy is a cloud-native, open source edge and service proxy. There is a crash at `QuicheDataReader::PeekVarInt62Length()`. It is caused by integer underflow in the `QuicStreamSequencerBuffer::PeekRegion()` implementation.	5.9	More Details
CVE-2024-32974	Envoy is a cloud-native, open source edge and service proxy. A crash was observed in `EnvoyQuicServerStream::OnInitialHeadersComplete()` with following call stack. It is a use-after-free caused by QUICHE continuing push request headers after `StopReading()` being called on the stream. As after `StopReading()`, the HCM's `ActiveStream` might have already be destroyed and any up calls from QUICHE could potentially cause use after free.	5.9	More Details
CVE-2024-34793	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kharim Tomlinson WP Next Post Navi allows Stored XSS.This issue affects WP Next Post Navi: from n/a through 1.8.3.	5.9	More Details
CVE-2024-34364	Envoy is a cloud-native, open source edge and service proxy. Envoy exposed an out-of-memory (OOM) vector from the mirror response, since async HTTP client will buffer the response with an unbounded buffer.	5.7	More Details
CVE-2024-36894	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_fs: Fix race between aio_cancel() and AIO request complete FFS based applications can utilize the aio_cancel() callback to dequeue pending USB requests submitted to the UDC. There is a scenario where the FFS application issues an AIO cancel call, while the UDC is handling a soft disconnect. For a DWC3 based implementation, the callstack looks like the following: DWC3 Gadget FFS Application dwc3_gadget_soft_disconnect() ... --> dwc3_stop_active_transfers() --> dwc3_gadget_giveback(-ESHUTDOWN) --> ffs_epfile_async_io_complete() ffs_aio_cancel() --> usb_ep_free_request() --> usb_ep_dequeue() There is currently no locking implemented between the AIO completion handler and AIO cancel, so the issue occurs if the completion routine is running in parallel to an AIO cancel call coming from the FFS application. As the completion call frees the USB request (io_data->req) the FFS application is also referencing it for the usb_ep_dequeue() call. This can lead to accessing a stale/hanging pointer. commit b566d38857fc ("usb: gadget: f_fs: use io_data->status consistently") relocated the usb_ep_free_request() into ffs_epfile_async_io_complete(). However, in order to properly implement locking to mitigate this issue, the spinlock can't be added to ffs_epfile_async_io_complete(), as usb_ep_dequeue() (if successfully dequeuing a USB request) will call the function driver's completion handler in the same context. Hence, leading into a deadlock. Fix this issue by moving the usb_ep_free_request() back to ffs_user_copy_worker(), and ensuring that it explicitly sets io_data->req to NULL after freeing it within the ffs->eps_lock. This resolves the race condition above, as the ffs_aio_cancel() routine will not continue attempting to dequeue a request that has already been freed, or the ffs_user_copy_work() not freeing the USB request until the AIO cancel is done referencing it. This fix depends on commit b566d38857fc ("usb: gadget: f_fs: use io_data->status consistently")	5.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36905	In the Linux kernel, the following vulnerability has been resolved: tcp: defer shutdown(SEND_SHUTDOWN) for TCP_SYN_RECV sockets TCP_SYN_RECV state is really special, it is only used by cross-syn connections, mostly used by fuzzers. In the following crash [1], syzbot managed to trigger a divide by zero in tcp_rcv_space_adjust() A socket makes the following state transitions, without ever calling tcp_init_transfer(), meaning tcp_init_buffer_space() is also not called. TCP_CLOSE connect() TCP_SYN_SENT TCP_SYN_RECV shutdown() -> tcp_shutdown(sk, SEND_SHUTDOWN) TCP_FIN_WAIT1 To fix this issue, change tcp_shutdown() to not perform a TCP_SYN_RECV -> TCP_FIN_WAIT1 transition, which makes no sense anyway. When tcp_rcv_state_process() later changes socket state from TCP_SYN_RECV to TCP_ESTABLISH, then look at sk->sk_shutdown to finally enter TCP_FIN_WAIT1 state, and send a FIN packet from a sane socket state. This means tcp_send_fin() can now be called from BH context, and must use GFP_ATOMIC allocations. [1] divide error: 0000 [#1] PREEMPT SMP KASAN NOPTI CPU: 1 PID: 5084 Comm: syz-executor358 Not tainted 6.9.0-rc6-syzkaller-00022-g98369dccd2f8 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 RIP: 0010:tcp_rcv_space_adjust+0x2df/0x890 net/ipv4/tcp_input.c:767 Code: e3 04 4c 01 eb 48 8b 44 24 38 0f b6 04 10 84 c0 49 89 d5 0f 85 a5 03 00 00 41 8b 8e c8 09 00 00 89 e8 29 c8 48 0f af c3 31 d2 <48> f7 f1 48 8d 1c 43 49 8d 96 76 08 00 00 48 89 d0 48 c1 e8 03 48 RSP: 0018:ffffc900031ef3f0 EFLAGS: 00010246 RAX: 0c677a10441f8f42 RBX: 000000004fb95e7e RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: 0000000027d4b11f R08: ffffffff89e535a4 R09: 1ffffffff25e6ab7 R10: dffffc0000000000 R11: ffffffff8135e920 R12: ffff88802a9f8d30 R13: dffffc0000000000 R14: ffff88802a9f8d00 R15: 1ffff1100553f2da FS: 00005555775c0380(0000) GS:ffff8880b9500000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f1155bf2304 CR3: 000000002b9f2000 CR4: 0000000000350ef0 Call Trace: <TASK> tcp_recvmsg_locked+0x106d/0x25a0 net/ipv4/tcp.c:2513 tcp_recvmsg+0x25d/0x920 net/ipv4/tcp.c:2578 inet6_recvmsg+0x16a/0x730 net/ipv6/af_inet6.c:680 sock_recvmsg_nosec net/socket.c:1046 [inline] sock_recvmsg+0x109/0x280 net/socket.c:1068 ____sys_recvmsg+0x1db/0x470 net/socket.c:2803 ___sys_recvmsg net/socket.c:2845 [inline] do_recvmmsg+0x474/0xae0 net/socket.c:2939 __sys_recvmmsg net/socket.c:3018 [inline] __do_sys_recvmmsg net/socket.c:3041 [inline] __se_sys_recvmmsg net/socket.c:3034 [inline] __x64_sys_recvmmsg+0x199/0x250 net/socket.c:3034 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf5/0x240 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7faeb6363db9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 c1 17 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:00007ffcc1997168 EFLAGS: 00000246 ORIG_RAX: 000000000000012b RAX: ffffffffffffffda RBX: 0000000000000000 RCX: 00007faeb6363db9 RDX: 0000000000000001 RSI: 0000000020000bc0 RDI: 0000000000000005 RBP: 0000000000000000 R08: 0000000000000000 R09: 000000000000001c R10: 0000000000000122 R11: 0000000000000246 R12: 0000000000000000 R13: 0000000000000000 R14: 0000000000000001 R15: 0000000000000001	5.5	More Details
CVE-2024-36891	In the Linux kernel, the following vulnerability has been resolved: maple_tree: fix mas_empty_area_rev() null pointer dereference Currently the code calls mas_start() followed by mas_data_end() if the maple state is MA_START, but mas_start() may return with the maple state node == NULL. This will lead to a null pointer dereference when checking information in the NULL node, which is done in mas_data_end(). Avoid setting the offset if there is no node by waiting until after the maple state is checked for an empty or single entry state. A user could trigger the events to cause a kernel oops by unmapping all vmas to produce an empty maple tree, then mapping a vma that would cause the scenario described above.	5.5	More Details
CVE-2022-28658	Apport argument parsing mishandles filename splitting on older kernels resulting in argument spoofing	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36893	In the Linux kernel, the following vulnerability has been resolved: usb: typec: tcpm: Check for port partner validity before consuming it typec_register_partner() does not guarantee partner registration to always succeed. In the event of failure, port->partner is set to the error value or NULL. Given that port->partner validity is not checked, this results in the following crash: Unable to handle kernel NULL pointer dereference at virtual address xx pc : run_state_machine+0x1bc8/0x1c08 lr : run_state_machine+0x1b90/0x1c08 .. Call trace: run_state_machine+0x1bc8/0x1c08 tcpm_state_machine_work+0x94/0xe4 kthread_worker_fn+0x118/0x328 kthread+0x1d0/0x23c ret_from_fork+0x10/0x20 To prevent the crash, check for port->partner validity before derefencing it in all the call sites.	5.5	More Details
CVE-2024-36926	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries/iommu: LPAR panics during boot up with a frozen PE At the time of LPAR boot up, partition firmware provides Open Firmware property ibm,dma-window for the PE. This property is provided on the PCI bus the PE is attached to. There are execptions where the partition firmware might not provide this property for the PE at the time of LPAR boot up. One of the scenario is where the firmware has frozen the PE due to some error condition. This PE is frozen for 24 hours or unless the whole system is reinitialized. Within this time frame, if the LPAR is booted, the frozen PE will be presented to the LPAR but ibm,dma-window property could be missing. Today, under these circumstances, the LPAR oopses with NULL pointer dereference, when configuring the PCI bus the PE is attached to. BUG: Kernel NULL pointer dereference on read at 0x000000c8 Faulting instruction address: 0xc0000000001024c0 Oops: Kernel access of bad area, sig: 7 [#1] LE PAGE_SIZE=64K MMU=Radix SMP NR_CPUS=2048 NUMA pSeries Modules linked in: Supported: Yes CPU: 0 PID: 1 Comm: swapper/0 Not tainted 6.4.0-150600.9-default #1 Hardware name: IBM,9043-MRX POWER10 (raw) 0x800200 0xf000006 of:IBM,FW1060.00 (NM1060_023) hv:phyp pSeries NIP: c0000000001024c0 LR: c0000000001024b0 CTR: c000000000102450 REGS: c0000000037db5c0 TRAP: 0300 Not tainted (6.4.0-150600.9-default) MSR: 8000000002009033 <SF,VEC,EE,ME,IR,DR,RI,LE> CR: 28000822 XER: 00000000 CFAR: c00000000010254c DAR: 00000000000000c8 DSISR: 00080000 IRQMASK: 0 ... NIP [c0000000001024c0] pci_dma_bus_setup_pSeriesLP+0x70/0x2a0 LR [c0000000001024b0] pci_dma_bus_setup_pSeriesLP+0x60/0x2a0 Call Trace: pci_dma_bus_setup_pSeriesLP+0x60/0x2a0 (unreliable) pcibios_setup_bus_self+0x1c0/0x370 __of_scan_bus+0x2f8/0x330 pcibios_scan_phb+0x280/0x3d0 pcibios_init+0x88/0x12c do_one_initcall+0x60/0x320 kernel_init_freeable+0x344/0x3e4 kernel_init+0x34/0x1d0 ret_from_kernel_user_thread+0x14/0x1c	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36884	In the Linux kernel, the following vulnerability has been resolved: iommu/arm-smmu: Use the correct type in nvidia_smmu_context_fault() This was missed because of the function pointer indirection. nvidia_smmu_context_fault() is also installed as a irq function, and the 'void *' was changed to a struct arm_smmu_domain. Since the iommu_domain is embedded at a non-zero offset this causes nvidia_smmu_context_fault() to miscompute the offset. Fixup the types. Unable to handle kernel NULL pointer dereference at virtual address 0000000000000120 Mem abort info: ESR = 0x0000000096000004 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x04: level 0 translation fault Data abort info: ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 CM = 0, WnR = 0, TnD = 0, TagAccess = 0 GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 user pgtable: 4k pages, 48-bit VAs, pgdp=0000000107c9f000 [0000000000000120] pgd=0000000000000000, p4d=0000000000000000 Internal error: Oops: 0000000096000004 [#1] SMP Modules linked in: CPU: 1 PID: 47 Comm: kworker/u25:0 Not tainted 6.9.0-0.rc7.58.eln136.aarch64 #1 Hardware name: Unknown NVIDIA Jetson Orin NX/NVIDIA Jetson Orin NX, BIOS 3.1-32827747 03/19/2023 Workqueue: events_unbound deferred_probe_work_func pstate: 604000c9 (nZCv daIF +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : nvidia_smmu_context_fault+0x1c/0x158 lr : __free_irq+0x1d4/0x2e8 sp : ffff80008044b6f0 x29: ffff80008044b6f0 x28: ffff000080a60b18 x27: ffffd32b5172e970 x26: 0000000000000000 x25: ffff0000802f5aac x24: ffff0000802f5a30 x23: ffff0000802f5b60 x22: 0000000000000057 x21: 0000000000000000 x20: ffff0000802f5a00 x19: ffff000087d4cd80 x18: ffffffffffffffff x17: 6234362066666666 x16: 6630303078302d30 x15: ffff00008156d888 x14: 0000000000000000 x13: ffff0000801db910 x12: ffff00008156d6d0 x11: 0000000000000003 x10: ffff0000801db918 x9 : ffffd32b50f94d9c x8 : 1fffe0001032fda1 x7 : ffff00008197ed00 x6 : 000000000000000f x5 : 000000000000010e x4 : 000000000000010e x3 : 0000000000000000 x2 : ffffd32b51720cd8 x1 : ffff000087e6f700 x0 : 0000000000000057 Call trace: nvidia_smmu_context_fault+0x1c/0x158 __free_irq+0x1d4/0x2e8 free_irq+0x3c/0x80 devm_free_irq+0x64/0xa8 arm_smmu_domain_free+0xc4/0x158 iommu_domain_free+0x44/0xa0 iommu_deinit_device+0xd0/0xf8 __iommu_group_remove_device+0xcc/0xe0 iommu_bus_notifier+0x64/0xa8 notifier_call_chain+0x78/0x148 blocking_notifier_call_chain+0x4c/0x90 bus_notify+0x44/0x70 device_del+0x264/0x3e8 pci_remove_bus_device+0x84/0x120 pci_remove_root_bus+0x5c/0xc0 dw_pcie_host_deinit+0x38/0xe0 tegra_pcie_config_rp+0xc0/0x1f0 tegra_pcie_dw_probe+0x34c/0x700 platform_probe+0x70/0xe8 really_probe+0xc8/0x3a0 __driver_probe_device+0x84/0x160 driver_probe_device+0x44/0x130 __device_attach_driver+0xc4/0x170 bus_for_each_drv+0x90/0x100 __device_attach+0xa8/0x1c8 device_initial_probe+0x1c/0x30 bus_probe_device+0xb0/0xc0 deferred_probe_work_func+0xbc/0x120 process_one_work+0x194/0x490 worker_thread+0x284/0x3b0 kthread+0xf4/0x108 ret_from_fork+0x10/0x20 Code: a9b97bfd 910003fd a9025bf5 f85a0035 (b94122a1)	5.5	More Details
CVE-2024-23107	An exposure of sensitive information to an unauthorized actor vulnerability [CWE-200] in FortiWeb version 7.4.0, version 7.2.4 and below, version 7.0.8 and below, 6.3 all versions may allow an authenticated attacker to read password hashes of other administrators via CLI commands.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36902	In the Linux kernel, the following vulnerability has been resolved: ipv6: fib6_rules: avoid possible NULL dereference in fib6_rule_action() syzbot is able to trigger the following crash [1], caused by unsafe ip6_dst_idev() use. Indeed ip6_dst_idev() can return NULL, and must always be checked. [1] Oops: general protection fault, probably for non-canonical address 0xdfffffc0000000000: 0000 [#1] PREEMPT SMP KASAN PTI KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007] CPU: 0 PID: 31648 Comm: syz-executor.0 Not tainted 6.9.0-rc4-next-20240417-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 RIP: 0010:__fib6_rule_action net/ipv6/fib6_rules.c:237 [inline] RIP: 0010:fib6_rule_action+0x241/0x7b0 net/ipv6/fib6_rules.c:267 Code: 02 00 00 49 8d 9f d8 00 00 00 48 89 d8 48 c1 e8 03 42 80 3c 20 00 74 08 48 89 df e8 f9 32 bf f7 48 8b 1b 48 89 d8 48 c1 e8 03 <42> 80 3c 20 00 74 08 48 89 df e8 e0 32 bf f7 4c 8b 03 48 89 ef 4c RSP: 0018:ffffc9000fc1f2f0 EFLAGS: 00010246 RAX: 0000000000000000 RBX: 0000000000000000 RCX: 1a772f98c8186700 RDX: 0000000000000003 RSI: ffffffff8bcac4e0 RDI: ffffffff8c1f9760 RBP: ffff8880673fb980 R08: ffffffff8fac15ef R09: 1ffffffff1f582bd R10: dffffc0000000000 R11: fffffbfff1f582be R12: dffffc0000000000 R13: 0000000000000080 R14: ffff888076509000 R15: ffff88807a029a00 FS: 00007f55e82ca6c0(0000) GS:ffff8880b9400000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000001b31d23000 CR3: 0000000022b66000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> fib_rules_lookup+0x62c/0xdb0 net/core/fib_rules.c:317 fib6_rule_lookup+0x1fd/0x790 net/ipv6/fib6_rules.c:108 ip6_route_output_flags_noref net/ipv6/route.c:2637 [inline] ip6_route_output_flags+0x38e/0x610 net/ipv6/route.c:2649 ip6_route_output include/net/ip6_route.h:93 [inline] ip6_dst_lookup_tail+0x189/0x11a0 net/ipv6/ip6_output.c:1120 ip6_dst_lookup_flow+0xb9/0x180 net/ipv6/ip6_output.c:1250 sctp_v6_get_dst+0x792/0x1e20 net/sctp/ipv6.c:326 sctp_transport_route+0x12c/0x2e0 net/sctp/transport.c:455 sctp_assoc_add_peer+0x614/0x15c0 net/sctp/associola.c:662 sctp_connect_new_asoc+0x31d/0x6c0 net/sctp/socket.c:1099 __sctp_connect+0x66d/0xe30 net/sctp/socket.c:1197 sctp_connect net/sctp/socket.c:4819 [inline] sctp_inet_connect+0x149/0x1f0 net/sctp/socket.c:4834 __sys_connect_file net/socket.c:2048 [inline] __sys_connect+0x2df/0x310 net/socket.c:2065 __do_sys_connect net/socket.c:2075 [inline] __se_sys_connect net/socket.c:2072 [inline] __x64_sys_connect+0x7a/0x90 net/socket.c:2072 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf5/0x240 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36901	In the Linux kernel, the following vulnerability has been resolved: ipv6: prevent NULL dereference in ip6_output() According to syzbot, there is a chance that ip6_dst_idev() returns NULL in ip6_output(). Most places in IPv6 stack deal with a NULL idev just fine, but not here. syzbot reported: general protection fault, probably for non-canonical address 0xdffffc00000000bc: 0000 [#1] PREEMPT SMP KASAN PTI KASAN: null-ptr-deref in range [0x00000000000005e0-0x00000000000005e7] CPU: 0 PID: 9775 Comm: syz-executor.4 Not tainted 6.9.0-rc5-syzkaller-00157-g6a30653b604a #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 RIP: 0010:ip6_output+0x231/0x3f0 net/ipv6/ip6_output.c:237 Code: 3c 1e 00 49 89 df 74 08 4c 89 ef e8 19 58 db f7 48 8b 44 24 20 49 89 45 00 49 89 c5 48 8d 9d e0 05 00 00 48 89 d8 48 c1 e8 03 <42> 0f b6 04 38 84 c0 4c 8b 74 24 28 0f 85 61 01 00 00 8b 1b 31 ff RSP: 0018:ffffc9000927f0d8 EFLAGS: 00010202 RAX: 00000000000000bc RBX: 00000000000005e0 RCX: 0000000000040000 RDX: ffffc900131f9000 RSI: 0000000000004f47 RDI: 0000000000004f48 RBP: 0000000000000000 R08: ffffffff8a1f0b9a R09: 1ffffffff1f51fad R10: dfffffc0000000000 R11: fffffbfff1f51fae R12: ffff8880293ec8c0 R13: ffff88805d7fc000 R14: 1ffff1100527d91a R15: dfffffc0000000000 FS: 00007f135c6856c0(0000) GS:ffff8880b9400000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000020000080 CR3: 0000000064096000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> NF_HOOK include/linux/netfilter.h:314 [inline] ip6_xmit+0xefe/0x17f0 net/ipv6/ip6_output.c:358 sctp_v6_xmit+0x9f2/0x13f0 net/sctp/ipv6.c:248 sctp_packet_transmit+0x26ad/0x2ca0 net/sctp/output.c:653 sctp_packet_singleton+0x22c/0x320 net/sctp/outqueue.c:783 sctp_outq_flush_ctrl net/sctp/outqueue.c:914 [inline] sctp_outq_flush+0x6d5/0x3e20 net/sctp/outqueue.c:1212 sctp_side_effects net/sctp/sm_sideeffect.c:1198 [inline] sctp_do_sm+0x59cc/0x60c0 net/sctp/sm_sideeffect.c:1169 sctp_primitive_ASSOCIATE+0x95/0xc0 net/sctp/primitive.c:73 __sctp_connect+0x9cd/0xe30 net/sctp/socket.c:1234 sctp_connect net/sctp/socket.c:4819 [inline] sctp_inet_connect+0x149/0x1f0 net/sctp/socket.c:4834 __sys_connect_file net/socket.c:2048 [inline] __sys_connect+0x2df/0x310 net/socket.c:2065 __do_sys_connect net/socket.c:2075 [inline] __se_sys_connect net/socket.c:2072 [inline] __x64_sys_connect+0x7a/0x90 net/socket.c:2072 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf5/0x240 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f	5.5	More Details
CVE-2024-36925	In the Linux kernel, the following vulnerability has been resolved: swiotlb: initialise restricted pool list_head when SWIOTLB_DYNAMIC=y Using restricted DMA pools (CONFIG_DMA_RESTRICTED_POOL=y) in conjunction with dynamic SWIOTLB (CONFIG_SWIOTLB_DYNAMIC=y) leads to the following crash when initialising the restricted pools at boot-time: l Unable to handle kernel NULL pointer dereference at virtual address 0000000000000008 l Internal error: Oops: 0000000096000005 [#1] PREEMPT SMP l pc : rmem_swiotlb_device_init+0xfc/0x1ec l lr : rmem_swiotlb_device_init+0xf0/0x1ec l Call trace: l rmem_swiotlb_device_init+0xfc/0x1ec l of_reserved_mem_device_init_by_idx+0x18c/0x238 l of_dma_configure_id+0x31c/0x33c l platform_dma_configure+0x34/0x80 faddr2line reveals that the crash is in the list validation code: include/linux/list.h:83 include/linux/rculist.h:79 include/linux/rculist.h:106 kernel/dma/swiotlb.c:306 kernel/dma/swiotlb.c:1695 because add_mem_pool() is trying to list_add_rcu() to a NULL 'mem->pools'. Fix the crash by initialising the 'mem->pools' list_head in rmem_swiotlb_device_init() before calling add_mem_pool().	5.5	More Details
CVE-2024-36897	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Atom Integrated System Info v2_2 for DCN35 New request from KMD/VBIOS in order to support new UMA carveout model. This fixes a null dereference from accessing Ctx->dc_bios->integrated_info while it was NULL. DAL parses through the BIOS and extracts the necessary integrated_info but was missing a case for the new BIOS version 2.3.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36881	In the Linux kernel, the following vulnerability has been resolved: mm/userfaultfd: reset ptes when close() for wr-protected ones Userfaultfd unregister includes a step to remove wr-protect bits from all the relevant pgtable entries, but that only covered an explicit UFFDIO_UNREGISTER ioctl, not a close() on the userfaultfd itself. Cover that too. This fixes a WARN trace. The only user visible side effect is the user can observe leftover wr-protect bits even if the user close()ed on an userfaultfd when releasing the last reference of it. However hopefully that should be harmless, and nothing bad should happen even if so. This change is now more important after the recent page-table-check patch we merged in mm-unstable (446dd9ad37d0 ("mm/page_table_check: support userfault wr-protect entries")), as we'll do sanity check on uffd-wp bits without vma context. So it's better if we can 100% guarantee no uffd-wp bit leftovers, to make sure each report will be valid.	5.5	More Details
CVE-2024-36938	In the Linux kernel, the following vulnerability has been resolved: bpf, skmsg: Fix NULL pointer dereference in sk_psock_skb_ingress_enqueue Fix NULL pointer data-races in sk_psock_skb_ingress_enqueue() which syzbot reported [1]. [1] BUG: KCSAN: data-race in sk_psock_drop / sk_psock_skb_ingress_enqueue write to 0xffff88814b3278b8 of 8 bytes by task 10724 on cpu 1: sk_psock_stop_verdict net/core/skmsg.c:1257 [inline] sk_psock_drop+0x13e/0x1f0 net/core/skmsg.c:843 sk_psock_put include/linux/skmsg.h:459 [inline] sock_map_close+0x1a7/0x260 net/core/sock_map.c:1648 unix_release+0x4b/0x80 net/unix/af_unix.c:1048 __sock_release net/socket.c:659 [inline] sock_close+0x68/0x150 net/socket.c:1421 __fput+0x2c1/0x660 fs/file_table.c:422 __fput_sync+0x44/0x60 fs/file_table.c:507 __do_sys_close fs/open.c:1556 [inline] __se_sys_close+0x101/0x1b0 fs/open.c:1541 __x64_sys_close+0x1f/0x30 fs/open.c:1541 do_syscall_64+0xd3/0x1d0 entry_SYSCALL_64_after_hwframe+0x6d/0x75 read to 0xffff88814b3278b8 of 8 bytes by task 10713 on cpu 0: sk_psock_data_ready include/linux/skmsg.h:464 [inline] sk_psock_skb_ingress_enqueue+0x32d/0x390 net/core/skmsg.c:555 sk_psock_skb_ingress_self+0x185/0x1e0 net/core/skmsg.c:606 sk_psock_verdict_apply net/core/skmsg.c:1008 [inline] sk_psock_verdict_recv+0x3e4/0x4a0 net/core/skmsg.c:1202 unix_read_skb net/unix/af_unix.c:2546 [inline] unix_stream_read_skb+0x9e/0xf0 net/unix/af_unix.c:2682 sk_psock_verdict_data_ready+0x77/0x220 net/core/skmsg.c:1223 unix_stream_sendmsg+0x527/0x860 net/unix/af_unix.c:2339 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x140/0x180 net/socket.c:745 ____sys_sendmsg+0x312/0x410 net/socket.c:2584 ___sys_sendmsg net/socket.c:2638 [inline] __sys_sendmsg+0x1e9/0x280 net/socket.c:2667 __do_sys_sendmsg net/socket.c:2676 [inline] __se_sys_sendmsg net/socket.c:2674 [inline] __x64_sys_sendmsg+0x46/0x50 net/socket.c:2674 do_syscall_64+0xd3/0x1d0 entry_SYSCALL_64_after_hwframe+0x6d/0x75 value changed: 0xffffffff83d7feb0 -> 0x0000000000000000 Reported by Kernel Concurrency Sanitizer on: CPU: 0 PID: 10713 Comm: syz-executor.4 Tainted: G W 6.8.0-syzkaller-08951-gfe46a7dd189e #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 02/29/2024 Prior to this, commit 4cd12c6065df ("bpf, sockmap: Fix NULL pointer dereference in sk_psock_verdict_data_ready()") fixed one NULL pointer similarly due to no protection of saved_data_ready. Here is another different caller causing the same issue because of the same reason. So we should protect it with sk_callback_lock read lock because the writer side in the sk_psock_drop() uses "write_lock_bh(&sk->sk_callback_lock);". To avoid errors that could happen in future, I move those two pairs of lock into the sk_psock_data_ready(), which is suggested by John Fastabend.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36930	In the Linux kernel, the following vulnerability has been resolved: spi: fix null pointer dereference within spi_sync If spi_sync() is called with the non-empty queue and the same spi_message is then reused, the complete callback for the message remains set while the context is cleared, leading to a null pointer dereference when the callback is invoked from spi_finalize_current_message(). With function inlining disabled, the call stack might look like this: _raw_spin_lock_irqsave from complete_with_flags+0x18/0x58 complete_with_flags from spi_complete+0x8/0xc spi_complete from spi_finalize_current_message+0xec/0x184 spi_finalize_current_message from spi_transfer_one_message+0x2a8/0x474 spi_transfer_one_message from __spi_pump_transfer_message+0x104/0x230 __spi_pump_transfer_message from __spi_transfer_message_noqueue+0x30/0xc4 __spi_transfer_message_noqueue from __spi_sync+0x204/0x248 __spi_sync from spi_sync+0x24/0x3c spi_sync from mcp251xfd_regmap_crc_read+0x124/0x28c [mcp251xfd] mcp251xfd_regmap_crc_read [mcp251xfd] from _regmap_raw_read+0xf8/0x154 _regmap_raw_read from _regmap_bus_read+0x44/0x70 _regmap_bus_read from _regmap_read+0x60/0xd8 _regmap_read from regmap_read+0x3c/0x5c regmap_read from mcp251xfd_alloc_can_err_skb+0x1c/0x54 [mcp251xfd] mcp251xfd_alloc_can_err_skb [mcp251xfd] from mcp251xfd_irq+0x194/0xe70 [mcp251xfd] mcp251xfd_irq [mcp251xfd] from irq_thread_fn+0x1c/0x78 irq_thread_fn from irq_thread+0x118/0x1f4 irq_thread from kthread+0xd8/0xf4 kthread from ret_from_fork+0x14/0x28 Fix this by also setting message->complete to NULL when the transfer is complete.	5.5	More Details
CVE-2022-28652	~/.config/apport/settings parsing is vulnerable to "billion laughs" attack	5.5	More Details
CVE-2024-36023	In the Linux kernel, the following vulnerability has been resolved: Julia Lawall reported this null pointer dereference, this should fix it.	5.5	More Details
CVE-2024-35228	Wagtail is an open source content management system built on Django. Due to an improperly applied permission check in the `wagtail.contrib.settings` module, a user with access to the Wagtail admin and knowledge of the URL of the edit view for a settings model can access and update that setting, even when they have not been granted permission over the model. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. Patched versions have been released as Wagtail 6.0.5 and 6.1.2. Wagtail releases prior to 6.0 are unaffected. Users are advised to upgrade. Site owners who are unable to upgrade to a patched version can avoid the vulnerability in `ModelViewSet` by registering the model as a snippet instead. No workaround is available for `wagtail.contrib.settings`.	5.5	More Details
CVE-2024-36944	In the Linux kernel, the following vulnerability has been resolved: Reapply "drm/qxl: simplify qxl_fence_wait" This reverts commit 07ed11afb68d94eadd4ffc082b97c2331307c5ea. Stephen Rostedt reports: "I went to run my tests on my VMs and the tests hung on boot up. Unfortunately, the most I ever got out was: [93.607888] Testing event system initcall: OK [93.667730] Running tests on all trace events: [93.669757] Testing all events: OK [95.631064] ------------[cut here]------------ Timed out after 60 seconds" and further debugging points to a possible circular locking dependency between the console_owner locking and the worker pool locking. Reverting the commit allows Steve's VM to boot to completion again. [This may obviously result in the "[TTM] Buffer eviction failed" messages again, which was the reason for that original revert. But at this point this seems preferable to a non-booting system...]	5.5	More Details
CVE-2022-28656	is_closing_session() allows users to consume RAM in the Apport process	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36932	In the Linux kernel, the following vulnerability has been resolved: thermal/debugfs: Prevent use-after-free from occurring after cdev removal Since thermal_debug_cdev_remove() does not run under cdev->lock, it can run in parallel with thermal_debug_cdev_state_update() and it may free the struct thermal_debugfs object used by the latter after it has been checked against NULL. If that happens, thermal_debug_cdev_state_update() will access memory that has been freed already causing the kernel to crash. Address this by using cdev->lock in thermal_debug_cdev_remove() around the cdev->debugfs value check (in case the same cdev is removed at the same time in two different threads) and its reset to NULL. Cc :6.8+ <stable@vger.kernel.org> # 6.8+	5.5	More Details
CVE-2022-28654	is_closing_session() allows users to fill up apport.log	5.5	More Details
CVE-2022-43575	IBM Aspera Console 3.4.0 through 3.4.2 PL5 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 238645.	5.4	More Details
CVE-2024-4379	The Premium Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Global Tooltip widget in all versions up to, and including, 4.10.31 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2024-2470	The Simple Ajax Chat WordPress plugin before 20240412 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	5.4	More Details
CVE-2024-35468	A SQL injection vulnerability in /hrm/index.php in SourceCodester Human Resource Management System 1.0 allows attackers to execute arbitrary SQL commands via the password parameter.	5.4	More Details
CVE-2023-40557	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in PickPlugins Tabs & Accordion allows Code Injection.This issue affects Tabs & Accordion: from n/a through 1.3.10.	5.4	More Details
CVE-2024-31889	IBM Planning Analytics Local 2.0 and 2.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 288136.	5.4	More Details
CVE-2024-31907	IBM Planning Analytics Local 2.0 and 2.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 289889.	5.4	More Details
CVE-2024-0756	The Insert or Embed Articulate Content into WordPress plugin through 4.3000000023 lacks validation of URLs when adding iframes, allowing attackers to inject an iFrame in the page and thus load arbitrary content from any page.	5.4	More Details
CVE-2022-25037	An issue in wanEditor v4.7.11 and fixed in v.4.7.12 and v.5 was discovered to contain a cross-site scripting (XSS) vulnerability via the image upload function.	5.4	More Details
CVE-2024-35351	A vulnerability has been discovered in Diño Physics School Assistant version 2.3. This vulnerability impacts unidentified code within the file /classes/SystemSettings.php?f=update_settings. Manipulating the parameter name results in cross-site scripting.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3190	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's text field widget in all versions up to, and including, 1.5.107 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Please note that this vulnerability is different in that the issue stems from an external template. It appears that older version may also be patched due to this, however, we are choosing 1.5.108 as the patched version since that is the most recent version containing as known patch.	5.4	More Details
CVE-2024-28103	Action Pack is a framework for handling and responding to web requests. Since 6.1.0, the application configurable Permissions-Policy is only served on responses with an HTML related Content-Type. This vulnerability is fixed in 6.1.7.8, 7.0.8.2, and 7.1.3.3.	5.4	More Details
CVE-2023-45635	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in WP Darko Responsive Tabs allows Code Injection.This issue affects Responsive Tabs: from n/a before 4.0.6.	5.4	More Details
CVE-2024-30889	Cross Site Scripting vulnerability in audimex audimexEE v.15.1.2 and fixed in 15.1.3.9 allows a remote attacker to execute arbitrary code via the service, method, widget_type, request_id, payload parameters.	5.4	More Details
CVE-2024-2089	The Remote Content Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'remote_content' shortcode in all versions up to, and including, 1.5 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.	5.4	More Details
CVE-2024-36366	In JetBrains TeamCity before 2022.04.7, 2022.10.6, 2023.05.6, 2023.11.5 an XSS could be executed via certain report grouping and filtering operations	5.4	More Details
CVE-2024-3269	The Download Monitor plugin for WordPress is vulnerable to unauthorized access to functionality due to a missing capability check on the dlm_uninstall_plugin function in all versions up to, and including, 4.9.13. This makes it possible for authenticated attackers to uninstall the plugin and delete its data.	5.4	More Details
CVE-2024-35345	A vulnerability has been discovered in Diño Physics School Assistant version 2.3. The vulnerability impacts unidentified code within the file /classes/Users.php. Manipulating the argument id results in cross-site scripting.	5.4	More Details
CVE-2023-39161	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in WP Discussion Board Discussion Board allows Content Spoofing, Cross-Site Scripting (XSS).This issue affects Discussion Board: from n/a through 2.4.8.	5.4	More Details
CVE-2024-30528	Missing Authorization vulnerability in Spiffy Plugins Spiffy Calendar.This issue affects Spiffy Calendar: from n/a through 4.9.10.	5.4	More Details
CVE-2023-47513	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in ARI Soft ARI Stream Quiz allows Code Injection.This issue affects ARI Stream Quiz: from n/a through 1.3.2.	5.4	More Details
CVE-2024-34754	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in A WP Life Contact Form Widget.This issue affects Contact Form Widget: from n/a through 1.3.9.	5.3	More Details
CVE-2023-34001	Improper Restriction of Excessive Authentication Attempts vulnerability in WPPlugins – WordPress Security Plugins Hide My WP Ghost allows Functionality Bypass.This issue affects Hide My WP Ghost: from n/a through 5.0.25.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37865	Authentication Bypass by Spoofing vulnerability in IP2Location Download IP2Location Country Blocker allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Download IP2Location Country Blocker: from n/a through 2.29.1.	5.3	More Details
CVE-2024-4997	The WPUpper Share Buttons plugin for WordPress is vulnerable to unauthorized access of data when preparing sharing links for posts and pages in all versions up to, and including, 3.43. This makes it possible for unauthenticated attackers to obtain the contents of password protected posts and pages.	5.3	More Details
CVE-2024-34798	Insertion of Sensitive Information into Log File vulnerability in Lukman Nakib Debug Log – Manger Tool.This issue affects Debug Log – Manger Tool: from n/a through 1.4.5.	5.3	More Details
CVE-2024-0434	The WordPress Tour & Travel Booking Plugin for WooCommerce – WpTravelly plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ttbm_new_place_save' function in all versions up to, and including, 1.7.1. This makes it possible for unauthenticated attackers to create and publish new place posts. This function is also vulnerable to CSRF.	5.3	More Details
CVE-2024-36124	iq80 Snappy is a compression/decompression library. When uncompressing certain data, Snappy tries to read outside the bounds of the given byte arrays. Because Snappy uses the JDK class `sun.misc.Unsafe` to speed up memory access, no additional bounds checks are performed and this has similar security consequences as out-of-bounds access in C or C++, namely it can lead to non-deterministic behavior or crash the JVM. iq80 Snappy is not actively maintained anymore. As quick fix users can upgrade to version 0.5.	5.3	More Details
CVE-2024-2382	The Authorize.net Payment Gateway For WooCommerce plugin for WordPress is vulnerable to payment bypass in all versions up to, and including, 8.0. This is due to the plugin not properly verifying the authenticity of the request that updates a orders payment status. This makes it possible for unauthenticated attackers to update order payment statuses to paid bypassing any payment.	5.3	More Details
CVE-2024-35670	Broken Authentication vulnerability in SoftLab Integrate Google Drive.This issue affects Integrate Google Drive: from n/a through 1.3.93.	5.3	More Details
CVE-2024-35357	A vulnerability has been discovered in Diño Physics School Assistant version 2.3. The vulnerability impacts an unidentified code within the file /classes/Master.php?f=delete_item. Manipulating the argument id can result in SQL injection.	5.3	More Details
CVE-2024-1718	The Claudio Sanches – Checkout Cielo for WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to insufficient payment validation in the update_order_status() function in all versions up to, and including, 1.1.0. This makes it possible for unauthenticated attackers to update the status of orders to paid bypassing payment.	5.3	More Details
CVE-2023-23738	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in Brainstorm Force Spectra allows Content Spoofing, Phishing.This issue affects Spectra: from n/a through 2.3.0.	5.3	More Details
CVE-2023-23735	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Brainstorm Force Spectra allows Code Injection.This issue affects Spectra: from n/a through 2.3.0.	5.3	More Details
CVE-2024-30525	Missing Authorization vulnerability in moveaddons Move Addons for Elementor.This issue affects Move Addons for Elementor: from n/a through 1.2.9.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23730	Improper Restriction of Excessive Authentication Attempts vulnerability in Brainstorm Force Spectra allows Functionality Bypass.This issue affects Spectra: from n/a through 2.3.0.	5.3	More Details
CVE-2024-34161	When NGINX Plus or NGINX OSS are configured to use the HTTP/3 QUIC module and the network infrastructure supports a Maximum Transmission Unit (MTU) of 4096 or greater without fragmentation, undisclosed QUIC packets can cause NGINX worker processes to leak previously freed memory.	5.3	More Details
CVE-2024-5524	Information exposure vulnerability in Astrotalks affecting version 10/03/2023. This vulnerability allows unregistered users to access all internal links of the application without providing any credentials.	5.3	More Details
CVE-2023-48318	Improper Restriction of Excessive Authentication Attempts vulnerability in CodePeople Contact Form Email allows Functionality Bypass.This issue affects Contact Form Email: from n/a through 1.3.41.	5.3	More Details
CVE-2024-36947	In the Linux kernel, the following vulnerability has been resolved: qibfs: fix dentry leak simple_recursive_removal() drops the pinning references to all positives in subtree. For the cases when its argument has been kept alive by the pinning alone that's exactly the right thing to do, but here the argument comes from dcache lookup, that needs to be balanced by explicit dput(). Fucked-up-by: Al Viro <viro@zeniv.linux.org.uk>	5.3	More Details
CVE-2023-48290	Improper Restriction of Excessive Authentication Attempts vulnerability in 10Web Form Builder Team Form Maker by 10Web allows Functionality Bypass.This issue affects Form Maker by 10Web: from n/a through 1.15.20.	5.3	More Details
CVE-2023-51542	Authentication Bypass by Spoofing vulnerability in WPMU DEV Branda allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Branda: from n/a through 3.4.14.	5.3	More Details
CVE-2023-48285	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Tips and Tricks HQ Stripe Payments allows Code Injection.This issue affects Stripe Payments: from n/a through 2.0.79.	5.3	More Details
CVE-2023-51543	Authentication Bypass by Spoofing vulnerability in Metagauss RegistrationMagic allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects RegistrationMagic: from n/a through 5.2.5.0.	5.3	More Details
CVE-2023-51544	Improper Control of Interaction Frequency vulnerability in Metagauss RegistrationMagic allows Functionality Misuse.This issue affects RegistrationMagic: from n/a through 5.2.5.0.	5.3	More Details
CVE-2023-51667	Authentication Bypass by Spoofing vulnerability in FeedbackWP Rate my Post – WP Rating System allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Rate my Post – WP Rating System: from n/a through 3.4.2.	5.3	More Details
CVE-2024-35512	An issue in hmq v1.5.5 allows attackers to cause a Denial of Service (DoS) via crafted requests.	5.3	More Details
CVE-2023-52176	Authentication Bypass by Spoofing vulnerability in miniorange Malware Scanner allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Malware Scanner: from n/a through 4.7.1.	5.3	More Details
CVE-2023-47189	Improper Authentication vulnerability in WPMU DEV Defender Security allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Defender Security: from n/a through 4.2.0.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1324	The QQWorld Auto Save Images plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the save_remote_images_get_auto_saved_results() function hooked via a norpriv AJAX in all versions up to, and including, 1.9.8. This makes it possible for unauthenticated attackers to retrieve the contents of arbitrary posts that may not be public.	5.3	More Details
CVE-2023-48753	Authentication Bypass by Spoofing vulnerability in 10up Restricted Site Access allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Restricted Site Access: from n/a through 7.4.1.	5.3	More Details
CVE-2023-48271	Authentication Bypass by Spoofing vulnerability in yonifre Maspik – Spam blacklist allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Maspik – Spam blacklist: from n/a through 0.10.3.	5.3	More Details
CVE-2023-46310	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in gVectors Team wpDiscuz allows Code Injection.This issue affects wpDiscuz: from n/a through 7.6.10.	5.3	More Details
CVE-2024-35200	When NGINX Plus or NGINX OSS are configured to use the HTTP/3 QUIC module, undisclosed HTTP/3 requests can cause NGINX worker processes to terminate.	5.3	More Details
CVE-2024-36375	In JetBrains TeamCity before 2024.03.2 technical information regarding TeamCity server could be exposed	5.3	More Details
CVE-2023-48745	Improper Restriction of Excessive Authentication Attempts vulnerability in WebFactory Ltd Captcha Code allows Functionality Bypass.This issue affects Captcha Code: from n/a through 2.9.	5.3	More Details
CVE-2024-5587	A vulnerability was found in Casdoor up to 1.335.0. It has been classified as problematic. Affected is an unknown function of the file /conf/app.conf of the component Configuration File Handler. The manipulation leads to files or directories accessible. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-266838 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2023-48276	Improper Restriction of Excessive Authentication Attempts vulnerability in Nitin Rathod WP Forms Puzzle Captcha allows Functionality Bypass.This issue affects WP Forms Puzzle Captcha: from n/a through 4.1.	5.3	More Details
CVE-2023-45009	Improper Restriction of Excessive Authentication Attempts vulnerability in Forge12 Interactive GmbH Captcha/Honeypot for Contact Form 7 allows Functionality Bypass.This issue affects Captcha/Honeypot for Contact Form 7: from n/a through 1.11.3.	5.3	More Details
CVE-2023-40332	Improper Control of Interaction Frequency vulnerability in Lester ‘GaMerZ’ Chan WP-PostRatings allows Functionality Misuse.This issue affects WP-PostRatings: from n/a through 1.91.	5.3	More Details
CVE-2023-49774	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in J.N. Breetvelt a.K.A. OpaJaap WP Photo Album Plus allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects WP Photo Album Plus: from n/a through 8.5.02.005.	5.3	More Details
CVE-2023-41134	Authentication Bypass by Spoofing vulnerability in pluginkollektiv Antispam Bee allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Antispam Bee: from n/a through 2.11.3.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44235	Improper Restriction of Excessive Authentication Attempts vulnerability in Devnath verma WP Captcha allows Functionality Bypass.This issue affects WP Captcha: from n/a through 2.0.0.	5.3	More Details
CVE-2024-20885	Improper component protection vulnerability in Samsung Dialer prior to SMR May-2024 Release 1 allows local attackers to make a call without proper permission.	5.1	More Details
CVE-2023-46297	An issue was discovered on Mercusys MW325R EU V3 MW325R(EU)_V3_1.11.0 221019 devices. A WAN attacker can make the admin interface unreachable/invisible via an unauthenticated HTTP request. Verification of the data sent by the user does not occur. The web server does not crash, but the admin interface becomes invisible, because the files necessary to display the content are no longer available. A reboot of the router is typically required to restore the correct behavior.	5.1	More Details
CVE-2024-20070	In modem, there is a possible information disclosure due to using risky cryptographic algorithm during connection establishment negotiation. This could lead to remote information disclosure, when weak encryption algorithm is used, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00942482; Issue ID: MSV-1469.	5.1	More Details
CVE-2024-3277	The Yumpu ePaper publishing plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the ajax_handler function in all versions up to, and including, 2.0.24. This makes it possible for authenticated attackers, with subscriber-level access and above, to upload PDF files and publish them, as well as modify the API key.	5.0	More Details
CVE-2024-35634	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Wow-Company Woocommerce – Recent Purchases allows PHP Local File Inclusion.This issue affects Woocommerce – Recent Purchases: from n/a through 1.0.1.	4.9	More Details
CVE-2024-31079	When NGINX Plus or NGINX OSS are configured to use the HTTP/3 QUIC module, undisclosed HTTP/3 requests can cause NGINX worker processes to terminate or cause other potential impact. This attack requires that a request be specifically timed during the connection draining process, which the attacker has no visibility and limited influence over.	4.8	More Details
CVE-2024-4219	Prior to 23.2, it is possible to perform arbitrary Server-Side requests via HTTP-based connectors within BeyondInsight, resulting in a server-side request forgery vulnerability.	4.8	More Details
CVE-2024-3921	The Gianism WordPress plugin through 5.1.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-36371	In JetBrains TeamCity before 2023.05.6, 2023.11.5 stored XSS in Commit status publisher was possible	4.6	More Details
CVE-2024-36370	In JetBrains TeamCity before 2022.04.7, 2022.10.6, 2023.05.6, 2023.11.5 stored XSS via OAuth connection settings was possible	4.6	More Details
CVE-2024-36369	In JetBrains TeamCity before 2022.04.7, 2022.10.6, 2023.05.6, 2023.11.5 stored XSS via issue tracker integration was possible	4.6	More Details
CVE-2024-20882	Out-of-bounds read vulnerability in bootloader prior to SMR June-2024 Release 1 allows physical attackers to arbitrary data access.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36372	In JetBrains TeamCity before 2023.05.6 reflected XSS on the subscriptions page was possible	4.6	More Details
CVE-2024-36373	In JetBrains TeamCity before 2024.03.2 several stored XSS in untrusted builds settings were possible	4.6	More Details
CVE-2024-36367	In JetBrains TeamCity before 2022.04.7, 2022.10.6, 2023.05.6, 2023.11.5 stored XSS via third-party reports was possible	4.6	More Details
CVE-2024-36374	In JetBrains TeamCity before 2024.03.2 stored XSS via build step settings was possible	4.6	More Details
CVE-2024-34051	A Reflected Cross-site scripting (XSS) vulnerability located in htdocs/compta/paiement/card.php of Dolibarr before 19.0.2 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into the facid parameter.	4.6	More Details
CVE-2024-36368	In JetBrains TeamCity before 2022.04.7, 2022.10.6, 2023.05.6, 2023.11.5 reflected XSS via OAuth provider configuration was possible	4.6	More Details
CVE-2023-47663	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Menno Luitjes Foyer allows Code Injection.This issue affects Foyer: from n/a through 1.7.5.	4.6	More Details
CVE-2024-36363	In JetBrains TeamCity before 2022.04.7, 2022.10.6, 2023.05.6, 2023.11.5 several Stored XSS in code inspection reports were possible	4.6	More Details
CVE-2022-43384	IBM Aspera Console 3.4.0 through 3.4.2 PL5 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 238645.	4.6	More Details
CVE-2024-36953	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: vgic-v2: Check for non-NULL vCPU in vgic_v2_parse_attr() vgic_v2_parse_attr() is responsible for finding the vCPU that matches the user-provided CPUID, which (of course) may not be valid. If the ID is invalid, kvm_get_vcpu_by_id() returns NULL, which isn't handled gracefully. Similar to the GICv3 uaccess flow, check that kvm_get_vcpu_by_id() actually returns something and fail the ioctl if not.	4.4	More Details
CVE-2024-35635	Server-Side Request Forgery (SSRF) vulnerability in WPManageNinja LLC Ninja Tables.This issue affects Ninja Tables: from n/a through 5.0.9.	4.4	More Details
CVE-2024-3031	The Fluid Notification Bar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.2.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2024-35637	Server-Side Request Forgery (SSRF) vulnerability in Church Admin.This issue affects Church Admin: from n/a through 4.3.6.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20071	In wlan driver, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00364733; Issue ID: MSV-1331.	4.4	More Details
CVE-2024-2657	The Font Farsi plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.6.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2024-3946	The WP To Do plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.3.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2024-4419	The Fetch JFT plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings 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 administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2024-4462	The Nafeza Prayer Time plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.2.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36928	In the Linux kernel, the following vulnerability has been resolved: s390/qeth: Fix kernel panic after setting hsuid Symptom: When the hsuid attribute is set for the first time on an IQD Layer3 device while the corresponding network interface is already UP, the kernel will try to execute a napi function pointer that is NULL. Example: ---------- [2057.572696] illegal operation: 0001 ilc:1 [#1] SMP [2057.572702] Modules linked in: af_iucv qeth_l3 zfcp scsi_transport_fc sunrpc nft_fib_inet nft_fib_ipv4 nft_fib_ipv6 nft_fib nft_reject_inet nf_reject_ipv4 nf_reject_ipv6 nft_reject nft_ct nf_tables_set nft_chain_nat nf_nat nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 ip_set nf_tables libcrc32c nfnetlink ghash_s390 prng xts aes_s390 des_s390 de s_generic sha3_512_s390 sha3_256_s390 sha512_s390 vfio_ccw vfio_mdev mdev vfio_iommu_type1 eadm_sch vfio ext4 mbcache jbd2 qeth_l2 bridge stp llc dasd_eckd_mod qeth dasd_mod qdio ccwgroup pkey zcrypt [2057.572739] CPU: 6 PID: 60182 Comm: stress_client Kdump: loaded Not tainted 4.18.0-541.el8.s390x #1 [2057.572742] Hardware name: IBM 3931 A01 704 (LPAR) [2057.572744] Krnl PSW : 0704f00180000000 0000000000000002 (0x2) [2057.572748] R:0 T:1 IO:1 EX:1 Key:0 M:1 W:0 P:0 AS:3 CC:3 PM:0 RI:0 EA:3 [2057.572751] Krnl GPRS: 0000000000000004 0000000000000000 00000000a3b008d8 0000000000000000 [2057.572754] 00000000a3b008d8 cb923a29c779abc5 0000000000000000 00000000814cfd80 [2057.572756] 000000000000012c 0000000000000000 00000000a3b008d8 00000000a3b008d8 [2057.572758] 00000000bab6d500 00000000814cfd80 0000000091317e46 00000000814cfc68 [2057.572762] Krnl Code:#0000000000000000: 0000 illegal >0000000000000002: 0000 illegal 0000000000000004: 0000 illegal 0000000000000006: 0000 illegal 0000000000000008: 0000 illegal 000000000000000a: 0000 illegal 000000000000000c: 0000 illegal 000000000000000e: 0000 illegal [2057.572800] Call Trace: [2057.572801] ([<00000000ec639700>] 0xec639700) [2057.572803] [<0000000913183e2>] net_rx_action+0x2ba/0x398 [2057.572809] [<0000000091515f76>] __do_softirq+0x11e/0x3a0 [2057.572813] [<0000000090ce160c>] do_softirq_own_stack+0x3c/0x58 [2057.572817] ([<0000000090d2cbd6>] do_softirq.part.1+0x56/0x60) [2057.572822] [<0000000090d2cc60>] __local_bh_enable_ip+0x80/0x98 [2057.572825] [<0000000091314706>] __dev_queue_xmit+0x2be/0xd70 [2057.572827] [<000003ff803dd6d6>] afiucv_hs_send+0x24e/0x300 [af_iucv] [2057.572830] [<000003ff803dd88a>] iucv_send_ctrl+0x102/0x138 [af_iucv] [2057.572833] [<000003ff803de72a>] iucv_sock_connect+0x37a/0x468 [af_iucv] [2057.572835] [<00000000912e7e90>] __sys_connect+0xa0/0xd8 [2057.572839] [<00000000912e9580>] sys_socketcall+0x228/0x348 [2057.572841] [<0000000091514e1a>] system_call+0x2a6/0x2c8 [2057.572843] Last Breaking-Event-Address: [2057.572844] [<0000000091317e44>] __napi_poll+0x4c/0x1d8 [2057.572846] [2057.572847] Kernel panic - not syncing: Fatal exception in interrupt ---------- Analysis: There is one napi structure per out_q: card->qdio.out_qs[i].napi The napi.poll functions are set during qeth_open(). Since commit 1cfef80d4c2b ("s390/qeth: Don't call dev_close/dev_open (DOWN/UP)") qeth_set_offline()/qeth_set_online() no longer call dev_close()/ dev_open(). So if qeth_free_qdio_queues() cleared card->qdio.out_qs[i].napi.poll while the network interface was UP and the card was offline, they are not set again. Reproduction: chzdev -e $devno layer2=0 ip link set dev $network_interface up echo 0 > /sys/bus/ccw ---truncated---	4.4	More Details
CVE-2024-35633	Server-Side Request Forgery (SSRF) vulnerability in CreativeThemes Blocksy Companion.This issue affects Blocksy Companion: from n/a through 2.0.42.	4.4	More Details
CVE-2023-28492	Missing Authorization vulnerability in CodePeople CP Multi View Event Calendar allows Functionality Misuse.This issue affects CP Multi View Event Calendar: from n/a through 1.4.10.	4.3	More Details
CVE-2023-28494	Missing Authorization vulnerability in CodePeople Contact Form Email allows Functionality Misuse.This issue affects Contact Form Email: from n/a through 1.3.31.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4220	Prior to 23.1, an information disclosure vulnerability exists within BeyondInsight which can allow an attacker to enumerate usernames.	4.3	More Details
CVE-2024-4427	The Comparison Slider plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on several AJAX actions in all versions up to, and including, 1.0.5. This makes it possible for authenticated attackers, with subscriber access or above, to change plugin settings and perform other actions such deleting sliders.	4.3	More Details
CVE-2024-4205	The Premium Addons for Elementor plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the get_template_content() function in all versions up to, and including, 4.10.31. This makes it possible for authenticated attackers, with subscriber-level access and above, to retrieve Elementor template data.	4.3	More Details
CVE-2024-4274	The Essential Real Estate plugin for WordPress is vulnerable to unauthorized loss of data due to insufficient validation on the remove_property_attachment_ajax() function in all versions up to, and including, 4.4.2. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary attachments.	4.3	More Details
CVE-2024-4355	The Block Bad Bots and Stop Bad Bots Crawlers and Spiders and Anti Spam Protection plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the stopbadbots_get_ajax_data() function in all versions up to, and including, 10.24. This makes it possible for authenticated attackers, with subscriber-level access and above, to expose visitor data.	4.3	More Details
CVE-2023-26523	Missing Authorization vulnerability in CodePeople Calculated Fields Form allows Functionality Misuse.This issue affects Calculated Fields Form: from n/a through 1.1.120.	4.3	More Details
CVE-2024-1717	The Admin Notices Manager plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the handle_ajax_call() function in all versions up to, and including, 1.4.0. This makes it possible for authenticated attackers, with subscriber-level access and above, to retrieve a list of registered user emails.	4.3	More Details
CVE-2023-27460	Missing Authorization vulnerability in CodePeople, paypaldev CP Contact Form with Paypal allows Functionality Misuse.This issue affects CP Contact Form with Paypal: from n/a through 1.3.34.	4.3	More Details
CVE-2024-35638	Cross-Site Request Forgery (CSRF) vulnerability in JumpDEMAND Inc. ActiveDEMAND.This issue affects ActiveDEMAND: from n/a through 0.2.43.	4.3	More Details
CVE-2024-4344	The Shield Security – Smart Bot Blocking & Intrusion Prevention Security plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 19.1.13. This is due to missing or incorrect nonce validation on the exec function. This makes it possible for unauthenticated attackers to disable pin protection for the admin interface of the plugin 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-2024-3945	The WP To Do plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.3.0. This is due to missing or incorrect nonce validation on the wptodo_manage() function. This makes it possible for unauthenticated attackers to add new todo items 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-2024-35636	Cross-Site Request Forgery (CSRF) vulnerability in Uploadcare Uploadcare File Uploader and Adaptive Delivery (beta) uploadcare.This issue affects Uploadcare File Uploader and Adaptive Delivery (beta): from n/a through 3.0.11.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-30484	Missing Authorization vulnerability in RT Easy Builder – Advanced addons for Elementor.This issue affects RT Easy Builder – Advanced addons for Elementor: from n/a through 2.0.	4.3	More Details
CVE-2024-3947	The WP To Do plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.3.0. This is due to missing or incorrect nonce validation on the wptodo_settings() function. This makes it possible for unauthenticated attackers to modify 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-2024-34006	The site log report required additional encoding of event descriptions to ensure any HTML in the content is displayed in plaintext instead of being rendered.	4.3	More Details
CVE-2023-26521	Missing Authorization vulnerability in CodePeople Search in Place allows Functionality Misuse.This issue affects Search in Place: from n/a through 1.0.104.	4.3	More Details
CVE-2024-34803	Missing Authorization vulnerability in Fastly.This issue affects Fastly: from n/a through 1.2.25.	4.3	More Details
CVE-2024-36845	An invalid pointer in the modbus_receive() function of libmodbus v3.1.6 allows attackers to cause a Denial of Service (DoS) via a crafted message sent to the unit-test-server.	4.3	More Details
CVE-2024-34000	ID numbers displayed in the lesson overview report required additional sanitizing to prevent a stored XSS risk.	4.3	More Details
CVE-2023-45053	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in pluginever WP Content Pilot – Autoblogging & Affiliate Marketing Plugin allows Code Injection.This issue affects WP Content Pilot – Autoblogging & Affiliate Marketing Plugin: from n/a through 1.3.3.	4.3	More Details
CVE-2024-3943	The WP To Do plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.3.0. This is due to missing or incorrect nonce validation on the wptodo_addcomment function. This makes it possible for unauthenticated attackers to add comments to to do items 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-2024-35632	Cross-Site Request Forgery (CSRF) vulnerability in CRM Perks. Integration for Contact Form 7 and Constant Contact.This issue affects Integration for Contact Form 7 and Constant Contact: from n/a through 1.1.5.	4.3	More Details
CVE-2024-4426	The Comparison Slider plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.5. This is due to missing or incorrect nonce validation on several functions hooked to AJAX actions. This makes it possible for unauthenticated attackers to change slider titles, delete sliders and modify plugin 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-2024-35221	Rubygems.org is the Ruby community's gem hosting service. A Gem publisher can cause a Remote DoS when publishing a Gem. This is due to how Ruby reads the Manifest of Gem files when using Gem::Specification.from_yaml. from_yaml makes use of SafeYAML.load which allows YAML aliases inside the YAML-based metadata of a gem. YAML aliases allow for Denial of Service attacks with so-called `YAML-bombs` (comparable to Billion laughs attacks). This was patched. There is is no action required by users. This issue is also tracked as GHSL-2024-001 and was discovered by the GitHub security lab.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48789	A client-side enforcement of server-side security in Fortinet FortiPortal version 6.0.0 through 6.0.14 allows attacker to improper access control via crafted HTTP requests.	4.3	More Details
CVE-2024-20873	Improper input validation vulnerability in caminfo driver prior to SMR Jun-2024 Release 1 allows local privileged attackers to write out-of-bounds memory.	4.2	More Details
CVE-2024-32877	Yii 2 is a PHP application framework. During internal penetration testing of a product based on Yii2, users discovered a Cross-site Scripting (XSS) vulnerability within the framework itself. This issue is relevant for the latest version of Yii2 (2.0.49.3). This issue lies in the mechanism for displaying function argument values in the stack trace. The vulnerability manifests when an argument's value exceeds 32 characters. For convenience, argument values exceeding this limit are truncated and displayed with an added "...". The full argument value becomes visible when hovering over it with the mouse, as it is displayed in the title attribute of a span tag. However, the use of a double quote (") allows an attacker to break out of the title attribute's value context and inject their own attributes into the span tag, including malicious JavaScript code through event handlers such as onmousemove. This vulnerability allows an attacker to execute arbitrary JavaScript code in the security context of the victim's site via a specially crafted link. This could lead to the theft of cookies (including httpOnly cookies, which are accessible on the page), content substitution, or complete takeover of user accounts. This issue has been addressed in version 2.0.50. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.2	More Details
CVE-2022-43841	IBM Aspera Console 3.4.0 through 3.4.2 PL9 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 239078.	4.0	More Details
CVE-2024-20065	In telephony, there is a possible information disclosure 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. Patch ID: ALPS08698617; Issue ID: MSV-1394.	4.0	More Details
CVE-2024-22338	IBM Security Verify Access OIDC Provider 22.09 through 23.03 could disclose sensitive information to a local user due to hazardous input validation. IBM X-Force ID: 279978.	4.0	More Details
CVE-2024-20875	Improper caller verification vulnerability in SemClipboard prior to SMR June-2024 Release 1 allows local attackers to access arbitrary files.	4.0	More Details
CVE-2024-20879	Improper input validation vulnerability in libsavscmn.so prior to SMR Jun-2024 Release 1 allows local attackers to write out-of-bounds memory.	4.0	More Details
CVE-2023-27437	Missing Authorization vulnerability in Event Espresso Event Espresso 4 Decaf allows Functionality Misuse.This issue affects Event Espresso 4 Decaf: from n/a through 4.10.44.Decaf.	3.7	More Details
CVE-2023-48335	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Webcraftic Hide login page allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Hide login page: from n/a through 1.1.9.	3.7	More Details
CVE-2023-52147	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in All In One WP Security & Firewall Team All In One WP Security & Firewall allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects All In One WP Security & Firewall: from n/a through 5.2.4.	3.7	More Details
CVE-2023-49741	Authentication Bypass by Spoofing vulnerability in wpdevart Coming soon and Maintenance mode allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Coming soon and Maintenance mode: from n/a through 3.7.3.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49748	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in WPServeur, NicolasKulka, wpformation WPS Hide Login allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects WPS Hide Login: from n/a through 1.9.11.	3.7	More Details
CVE-2023-47769	Authentication Bypass by Spoofing vulnerability in WP Maintenance allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects WP Maintenance: from n/a through 6.1.3.	3.7	More Details
CVE-2023-49822	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in David Vongries Ultimate Dashboard allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Ultimate Dashboard: from n/a through 3.7.10.	3.7	More Details
CVE-2023-24373	External Control of Assumed-Immutable Web Parameter vulnerability in WpDevArt Booking calendar, Appointment Booking System allows Manipulating Hidden Fields.This issue affects Booking calendar, Appointment Booking System: from n/a through 3.2.3.	3.7	More Details
CVE-2023-47818	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in LWS LWS Hide Login allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects LWS Hide Login: from n/a through 2.1.8.	3.7	More Details
CVE-2024-5437	A vulnerability was found in SourceCodester Simple Online Bidding System 1.0. It has been classified as problematic. Affected is the function save_category of the file /admin/index.php?page=categories. The manipulation of the argument 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. VDB-266442 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-31684	Incorrect access control in the fingerprint authentication mechanism of Bitdefender Mobile Security v4.11.3-gms allows attackers to bypass fingerprint authentication due to the use of a deprecated API.	3.5	More Details
CVE-2024-36118	MeterSphere is a test management and interface testing tool. In affected versions users without workspace permissions can view functional test cases of other workspaces beyond their authority. This issue has been addressed in version 2.10.15-lts. Users of MeterSphere are advised to upgrade. There are no known workarounds for this vulnerability.	3.5	More Details
CVE-2024-35311	Yubico YubiKey 5 Series before 5.7.0, Security Key Series before 5.7.0, YubiKey Bio Series before 5.6.4, and YubiKey 5 FIPS before 5.7.2 have Incorrect Access Control.	3.3	More Details
CVE-2024-34715	Fides is an open-source privacy engineering platform. The Fides webserver requires a connection to a hosted PostgreSQL database for persistent storage of application data. If the password used by the webserver for this database connection includes special characters such as `@` and `$`, webserver startup fails and the part of the password following the special character is exposed in webserver error logs. This is caused by improper escaping of the SQLAlchemy password string. As a result users are subject to a partial exposure of hosted database password in webserver logs. The vulnerability has been patched in Fides version `2.37.0`. Users are advised to upgrade to this version or later to secure their systems against this threat. There are no known workarounds for this vulnerability.	2.3	More Details
CVE-2024-36032	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: qca: fix info leak when fetching fw build id Add the missing sanity checks and move the 255-byte build-id buffer off the stack to avoid leaking stack data through debugfs in case the build-info reply is malformed.	2.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35196	Sentry is a developer-first error tracking and performance monitoring platform. Sentry's Slack integration incorrectly records the incoming request body in logs. This request data can contain sensitive information, including the deprecated Slack verification token. With this verification token, it is possible under specific configurations, an attacker can forge requests and act as the Slack integration. The request body is leaked in log entries matching `event == "slack.*" && name == "sentry.integrations.slack" && request_data == *`. The deprecated slack verification token, will be found in the `request_data.token` key. **SaaS users** do not need to take any action. **Self-hosted users** should upgrade to version 24.5.0 or higher, rotate their Slack verification token, and use the Slack Signing Secret instead of the verification token. For users only using the `slack.signing-secret` in their self-hosted configuration, the legacy verification token is not used to verify the webhook payload. It is ignored. Users unable to upgrade should either set the `slack.signing-secret` instead of `slack.verification-token`. The signing secret is Slack's recommended way of authenticating webhooks. By having `slack.singing-secret` set, Sentry self-hosted will no longer use the verification token for authentication of the webhooks, regardless of whether `slack.verification-token` is set or not. Alternatively if the self-hosted instance is unable to be upgraded or re-configured to use the `slack.signing-secret`, the logging configuration can be adjusted to not generate logs from the integration. The default logging configuration can be found in `src/sentry/conf/server.py`. **Services should be restarted once the configuration change is saved.**	2.0	More Details
CVE-2024-36119	Statamic is a, Laravel + Git powered CMS designed for building websites. In affected versions users registering via the `user:register_form` tag will have their password confirmation stored in plain text in their user file. This only affects sites matching **all** of the following conditions: 1. Running Statamic versions between 5.3.0 and 5.6.1. (This version range represents only one calendar week), 2. Using the `user:register_form` tag. 3. Using file-based user accounts. (Does not affect users stored in a database.), 4. Has users that have registered during that time period. (Existing users are not affected.). Additionally passwords are only visible to users that have access to read user yaml files, typically developers of the application itself. This issue has been patched in version 5.6.2, however any users registered during that time period and using the affected version range will still have the the `password_confirmation` value in their yaml files. We recommend that affected users have their password reset. System administrators are advised to upgrade their deployments. There are no known workarounds for this vulnerability. Anyone who commits their files to a public git repo, may consider clearing the sensitive data from the git history as it is likely that passwords were uploaded.	1.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36906	In the Linux kernel, the following vulnerability has been resolved: ARM: 9381/1: kasan: clear stale stack poison We found below OOB crash: [33.452494] == [33.453513] BUG: KASAN: stack-out-of-bounds in refresh_cpu_vm_stats.constprop.0+0xcc/0x2ec [33.454660] Write of size 164 at addr c1d03d30 by task swapper/0/0 [33.455515] [33.455767] CPU: 0 PID: 0 Comm: swapper/0 Tainted: G O 6.1.25-mainline #1 [33.456880] Hardware name: Generic DT based system [33.457555] unwind_backtrace from show_stack+0x18/0x1c [33.458326] show_stack from dump_stack_lvl+0x40/0x4c [33.459072] dump_stack_lvl from print_report+0x158/0x4a4 [33.459863] print_report from kasan_report+0x9c/0x148 [33.460616] kasan_report from kasan_check_range+0x94/0x1a0 [33.461424] kasan_check_range from memset+0x20/0x3c [33.462157] memset from refresh_cpu_vm_stats.constprop.0+0xcc/0x2ec [33.463064] refresh_cpu_vm_stats.constprop.0 from tick_nohz_idle_stop_tick+0x180/0x53c [33.464181] tick_nohz_idle_stop_tick from do_idle+0x264/0x354 [33.465029] do_idle from cpu_startup_entry+0x20/0x24 [33.465769] cpu_startup_entry from rest_init+0xf0/0xf4 [33.466528] rest_init from arch_post_acpi_subsys_init+0x0/0x18 [33.467397] [33.467644] The buggy address belongs to stack of task swapper/0/0 [33.468493] and is located at offset 112 in frame: [33.469172] refresh_cpu_vm_stats.constprop.0+0x0/0x2ec [33.469917] [33.470165] This frame has 2 objects: [33.470696] [32, 76) 'global_zone_diff' [33.470729] [112, 276) 'global_node_diff' [33.471294] [33.472095] The buggy address belongs to the physical page: [33.472862] page:3cd72da8 refcount:1 mapcount:0 mapping:00000000 index:0x0 pfn:0x41d03 [33.473944] flags: 0x1000(reservedlzone=0) [33.474565] raw: 00001000 ed741470 ed741470 00000000 00000000 00000000 ffffffff 00000001 [33.475656] raw: 00000000 [33.476050] page dumped because: kasan: bad access detected [33.476816] [33.477061] Memory state around the buggy address: [33.477732] c1d03c00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [33.478630] c1d03c80: 00 00 00 00 00 00 00 00 f1 f1 f1 f1 00 00 00 00 [33.479526] >c1d03d00: 00 04 f2 f2 f2 f2 00 00 00 00 00 00 f1 f1 f1 f1 [33.480415] ^ [33.481195] c1d03d80: 00 00 00 00 00 00 00 00 00 00 04 f3 f3 f3 f3 f3 [33.482088] c1d03e00: f3 f3 f3 f3 00 00 00 00 00 00 00 00 00 00 00 00 [33.482978] == We find the root cause of this OOB is that arm does not clear stale stack poison in the case of cpuidle. This patch refer to arch/arm64/kernel/sleep.S to resolve this issue. From cited commit [1] that explain the problem Functions which the compiler has instrumented for KASAN place poison on the stack shadow upon entry and remove this poison prior to returning. In the case of cpuidle, CPUs exit the kernel a number of levels deep in C code. Any instrumented functions on this critical path will leave portions of the stack shadow poisoned. If CPUs lose context and return to the kernel via a cold path, we restore a prior context saved in __cpu_suspend_enter are forgotten, and we never remove the poison they placed in the stack shadow area by functions calls between this and the actual exit of the kernel. Thus, (depending on stackframe layout) subsequent calls to instrumented functions may hit this stale poison, resulting in (spurious) KASAN splats to the console. To avoid this, clear any stale poison from the idle thread for a CPU prior to bringing a CPU online. From cited commit [2] Extend to check for CONFIG_KASAN_STACK [1] commit 0d97e6d8024c ("arm64: kasan: clear stale stack poison") [2] commit d56a9ef84bd0 ("kasan, arm64: unpoison stack only with CONFIG_KASAN_STACK")	N/A	More Details
CVE-2024-36914	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Skip on writeback when it's not applicable [WHY] dynamic memory safety error detector (KASAN) catches and generates error messages "BUG: KASAN: slab-out-of-bounds" as writeback connector does not support certain features which are not initialized. [HOW] Skip them when connector type is DRM_MODE_CONNECTOR_WRITEBACK.	N/A	More Details
CVE-2024-36911	In the Linux kernel, the following vulnerability has been resolved: hv_netvsc: Don't free decrypted memory In CoCo VMs it is possible for the untrusted host to cause set_memory_encrypted() or set_memory_decrypted() to fail such that an error is returned and the resulting memory is shared. Callers need to take care to handle these errors to avoid returning decrypted (shared) memory to the page allocator, which could lead to functional or security issues. The netvsc driver could free decrypted/shared pages if set_memory_decrypted() fails. Check the decrypted field in the gpadl to decide whether to free the memory.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36909	In the Linux kernel, the following vulnerability has been resolved: Drivers: hv: vmbus: Don't free ring buffers that couldn't be re-encrypted In CoCo VMs it is possible for the untrusted host to cause set_memory_encrypted() or set_memory_decrypted() to fail such that an error is returned and the resulting memory is shared. Callers need to take care to handle these errors to avoid returning decrypted (shared) memory to the page allocator, which could lead to functional or security issues. The VMBus ring buffer code could free decrypted/shared pages if set_memory_decrypted() fails. Check the decrypted field in the struct vmbus_gpadl for the ring buffers to decide whether to free the memory.	N/A	More Details
CVE-2024-36907	In the Linux kernel, the following vulnerability has been resolved: SUNRPC: add a missing rpc_stat for TCP TLS Commit 1548036ef120 ("nfs: make the rpc_stat per net namespace") added functionality to specify rpc_stats function but missed adding it to the TCP TLS functionality. As the result, mounting with xprtsec=tls lead to the following kernel oops. [128.984192] Unable to handle kernel NULL pointer dereference at virtual address 000000000000001c [128.985058] Mem abort info: [128.985372] ESR = 0x0000000096000004 [128.985709] EC = 0x25: DABT (current EL), IL = 32 bits [128.986176] SET = 0, FnV = 0 [128.986521] EA = 0, S1PTW = 0 [128.986804] FSC = 0x04: level 0 translation fault [128.987229] Data abort info: [128.987597] ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 [128.988169] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [128.988811] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [128.989302] user pgtable: 4k pages, 48-bit VAs, pgdp=0000000106c84000 [128.990048] [000000000000001c] pgd=0000000000000000, p4d=0000000000000000 [128.990736] Internal error: Oops: 0000000096000004 [#1] SMP [128.991168] Modules linked in: nfs_layout_nfsv41_files rpcsec_gss_krb5 auth_rpcgss nfsv4 dns_resolver nfs lockd grace netfs uinput dm_mod nft_fib_inet nft_fib_ipv4 nft_fib_ipv6 nft_fib nft_reject_inet nf_reject_ipv4 nf_reject_ipv6 nft_reject nft_ct nft_chain_nat nf_nat nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 rfkill ip_set nf_tables nfnetlink qrtr vsock_loopback vmw_vsock_virtio_transport_common vmw_vsock_vmci_transport vsock sunrpc vfat fat uvcvideo videobuf2_vmalloc videobuf2_memops uvc videobuf2_v4l2 videodev videobuf2_common mc vmw_vmci xfs libcrc32c e1000e crct10dif_ce ghash_ce sha2_ce vmwgfx nvme sha256_arm64 nvme_core sr_mod cdrom sha1_ce drm_ttm_helper ttm drm_kms_helper drm sg fuse [128.996466] CPU: 0 PID: 179 Comm: kworker/u4:26 Kdump: loaded Not tainted 6.8.0-rc6+ #12 [128.997226] Hardware name: VMware, Inc. VMware20,1/VBSA, BIOS VMW201.00V.21805430.BA64.2305221830 05/22/2023 [128.998084] Workqueue: xprtiod xs_tcp_tls_setup_socket [sunrpc] [128.998701] pstate: 81400005 (Nzcv daif +PAN -UAO -TCO +DIT -SSBS BTYPE=--) [128.999384] pc : call_start+0x74/0x138 [sunrpc] [128.999809] lr : __rpc_execute+0xb8/0x3e0 [sunrpc] [129.000244] sp : ffff8000832b3a00 [129.000508] x29: ffff8000832b3a00 x28: ffff800081ac79c0 x27: ffff800081ac7000 [129.001111] x26: 0000000004248060 x25: 0000000000000000 x24: ffff800081596008 [129.001757] x23: ffff80007b087240 x22: ffff00009a509d30 x21: 0000000000000000 [129.002345] x20: ffff000090075600 x19: ffff00009a509d00 x18: ffffffffffffffff [129.002912] x17: 733d4d4554535953 x16: 42555300312d746e x15: ffff8000832b3a88 [129.003464] x14: ffffffffffffffff x13: ffff8000832b3a7d x12: 0000000000000008 [129.004021] x11: 0101010101010101 x10: ffff8000150cb560 x9 : ffff80007b087c00 [129.004577] x8 : ffff00009a509de0 x7 : 0000000000000000 x6 : 00000000be8c4ee3 [129.005026] x5 : 0000000000000000 x4 : 0000000000000000 x3 : ffff000094d56680 [129.005425] x2 : ffff80007b0637f8 x1 : ffff000090075600 x0 : ffff00009a509d00 [129.005824] Call trace: [129.005967] call_start+0x74/0x138 [sunrpc] [129.006233] __rpc_execute+0xb8/0x3e0 [sunrpc] [129.006506] rpc_execute+0x160/0x1d8 [sunrpc] [129.006778] rpc_run_task+0x148/0x1f8 [sunrpc] [129.007204] tls_probe+0x80/0xd0 [sunrpc] [129.007460] rpc_ping+0x28/0x80 [sunrpc] [129.007715] rpc_create_xprt+0x134/0x1a0 [sunrpc] [129.007999] rpc_create+0x128/0x2a0 [sunrpc] [129.008264] xs_tcp_tls_setup_socket+0xdc/0x508 [sunrpc] [129.008583] process_one_work+0x174/0x3c8 [129.008813] worker_thread+0x2c8/0x3e0 [129.009033] kthread+0x100/0x110 [129.009225] ret_from_fork+0x10/0x20 [129.009432] Code: f0ffffc2 911fe042 aa1403e1 aa1303e0 (b9401c83)	N/A	More Details
CVE-2024-4857	The FS Product Inquiry WordPress plugin through 1.1.1 does not sanitise and escape some form submissions, which could allow unauthenticated users to perform Stored Cross-Site Scripting attacks	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36904	In the Linux kernel, the following vulnerability has been resolved: tcp: Use refcount_inc_not_zero() in tcp_twsk_unique(). Anderson Nascimento reported a use-after-free splat in tcp_twsk_unique() with nice analysis. Since commit ec94c2696f0b ("tcp/dccp: avoid one atomic operation for timewait hashdance"), inet_twsk_hashdance() sets TIME-WAIT socket's sk_refcnt after putting it into ehash and releasing the bucket lock. Thus, there is a small race window where other threads could try to reuse the port during connect() and call sock_hold() in tcp_twsk_unique() for the TIME-WAIT socket with zero refcnt. If that happens, the refcnt taken by tcp_twsk_unique() is overwritten and sock_put() will cause underflow, triggering a real use-after-free somewhere else. To avoid the use-after-free, we need to use refcount_inc_not_zero() in tcp_twsk_unique() and give up on reusing the port if it returns false. [0]: refcount_t: addition on 0; use-after-free. WARNING: CPU: 0 PID: 1039313 at lib/refcount.c:25 refcount_warn_saturate+0xe5/0x110 CPU: 0 PID: 1039313 Comm: trigger Not tainted 6.8.6-200.fc39.x86_64 #1 Hardware name: VMware, Inc. VMware20,1/440BX Desktop Reference Platform, BIOS VMW201.00V.21805430.B64.2305221830 05/22/2023 RIP: 0010:refcount_warn_saturate+0xe5/0x110 Code: 42 8e ff 0f 0b c3 cc cc cc cc 80 3d aa 13 ea 01 00 0f 85 5e ff ff ff 48 c7 c7 f8 8e b7 82 c6 05 96 13 ea 01 01 e8 7b 42 8e ff <0f> 0b c3 cc cc cc cc 48 c7 c7 50 8f b7 82 c6 05 7a 13 ea 01 01 e8 RSP: 0018:ffffc90006b43b60 EFLAGS: 00010282 RAX: 0000000000000000 RBX: ffff888009bb3ef0 RCX: 0000000000000027 RDX: ffff88807be218c8 RSI: 0000000000000001 RDI: ffff88807be218c0 RBP: 0000000000069d70 R08: 0000000000000000 R09: ffffc90006b439f0 R10: ffffc90006b439e8 R11: 0000000000000003 R12: ffff8880029ede84 R13: 0000000000004e20 R14: ffffffff84356dc0 R15: ffff888009bb3ef0 FS: 00007f62c10926c0(0000) GS:ffff88807be00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000020ccb000 CR3: 000000004628c005 CR4: 0000000000f70ef0 PKRU: 55555554 Call Trace: <TASK> ? refcount_warn_saturate+0xe5/0x110 ? __warn+0x81/0x130 ? refcount_warn_saturate+0xe5/0x110 ? report_bug+0x171/0x1a0 ? refcount_warn_saturate+0xe5/0x110 ? handle_bug+0x3c/0x80 ? exc_invalid_op+0x17/0x70 ? asm_exc_invalid_op+0x1a/0x20 ? refcount_warn_saturate+0xe5/0x110 tcp_twsk_unique+0x186/0x190 __inet_check_established+0x176/0x2d0 __inet_hash_connect+0x74/0x7d0 ? __pfx___inet_check_established+0x10/0x10 tcp_v4_connect+0x278/0x530 __inet_stream_connect+0x10f/0x3d0 inet_stream_connect+0x3a/0x60 __sys_connect+0xa8/0xd0 __x64_sys_connect+0x18/0x20 do_syscall_64+0x83/0x170 entry_SYSCALL_64_after_hwframe+0x78/0x80 RIP: 0033:0x7f62c11a885d Code: ff c3 66 2e 0f 1f 84 00 00 00 00 00 90 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 a3 45 0c 00 f7 d8 64 89 01 48 RSP: 002b:00007f62c1091e58 EFLAGS: 00000296 ORIG_RAX: 000000000000002a RAX: ffffffffffffffda RBX: 0000000020ccb004 RCX: 00007f62c11a885d RDX: 0000000000000010 RSI: 0000000020ccb000 RDI: 0000000000000003 RBP: 00007f62c1091e90 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000296 R12: 00007f62c10926c0 R13: ffffffffffffff88 R14: 0000000000000000 R15: 00007ffe237885b0 </TASK>	N/A	More Details
CVE-2024-36903	In the Linux kernel, the following vulnerability has been resolved: ipv6: Fix potential uninit-value access in __ip6_make_skb() As it was done in commit fc1092f51567 ("ipv4: Fix uninit-value access in __ip_make_skb()") for IPv4, check FLOWI_FLAG_KNOWN_NH on fl6->flowi6_flags instead of testing HDRINCL on the socket to avoid a race condition which causes uninit-value access.	N/A	More Details
CVE-2024-36900	In the Linux kernel, the following vulnerability has been resolved: net: hns3: fix kernel crash when devlink reload during initialization The devlink reload process will access the hardware resources, but the register operation is done before the hardware is initialized. So, processing the devlink reload during initialization may lead to kernel crash. This patch fixes this by registering the devlink after hardware initialization.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36899	In the Linux kernel, the following vulnerability has been resolved: gpiolib: cdev: Fix use after free in lineinfo_changed_notify The use-after-free issue occurs as follows: when the GPIO chip device file is being closed by invoking gpio_chrdev_release(), watched_lines is freed by bitmap_free(), but the unregistration of lineinfo_changed_nb notifier chain failed due to waiting write rwsem. Additionally, one of the GPIO chip's lines is also in the release process and holds the notifier chain's read rwsem. Consequently, a race condition leads to the use-after-free of watched_lines. Here is the typical stack when issue happened: [free] gpio_chrdev_release() --> bitmap_free(cdev->watched_lines) <-- freed --> blocking_notifier_chain_unregister() --> down_write(&nh->rwsem) <-- waiting rwsem --> __down_write_common() --> rwsem_down_write_slowpath() --> schedule_preempt_disabled() --> schedule() [use] st54spi_gpio_dev_release() --> gpio_free() --> gpiod_free() --> gpiod_free_commit() --> gpiod_line_state_notify() --> blocking_notifier_call_chain() --> down_read(&nh->rwsem); <-- held rwsem --> notifier_call_chain() --> lineinfo_changed_notify() --> test_bit(xxxx, cdev->watched_lines) <-- use after free The side effect of the use-after-free issue is that a GPIO line event is being generated for userspace where it shouldn't. However, since the chrdev is being closed, userspace won't have the chance to read that event anyway. To fix the issue, call the bitmap_free() function after the unregistration of lineinfo_changed_nb notifier chain.	N/A	More Details
CVE-2024-36898	In the Linux kernel, the following vulnerability has been resolved: gpiolib: cdev: fix uninitialised kfifo If a line is requested with debounce, and that results in debouncing in software, and the line is subsequently reconfigured to enable edge detection then the allocation of the kfifo to contain edge events is overlooked. This results in events being written to and read from an uninitialised kfifo. Read events are returned to userspace. Initialise the kfifo in the case where the software debounce is already active.	N/A	More Details
CVE-2024-36895	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: uvc: use correct buffer size when parsing configfs lists This commit fixes uvc gadget support on 32-bit platforms. Commit 0df28607c5cb ("usb: gadget: uvc: Generalise helper functions for reuse") introduced a helper function __uvcg_iter_item_entries() to aid with parsing lists of items on configfs attributes stores. This function is a generalization of another very similar function, which used a stack-allocated temporary buffer of fixed size for each item in the list and used the sizeof() operator to check for potential buffer overruns. The new function was changed to allocate the now variably sized temp buffer on heap, but wasn't properly updated to also check for max buffer size using the computed size instead of sizeof() operator. As a result, the maximum item size was 7 (plus null terminator) on 64-bit platforms, and 3 on 32-bit ones. While 7 is accidentally just barely enough, 3 is definitely too small for some of UVC configfs attributes. For example, dwFrameInteval, specified in 100ns units, usually has 6-digit item values, e.g. 166666 for 60fps.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36915	In the Linux kernel, the following vulnerability has been resolved: nfc: llcp: fix nfc_llcp_setsockopt() unsafe copies syzbot reported unsafe calls to copy_from_sockptr() [1] Use copy_safe_from_sockptr() instead. [1] BUG: KASAN: slab-out-of-bounds in copy_from_sockptr_offset include/linux/sockptr.h:49 [inline] BUG: KASAN: slab-out-of-bounds in copy_from_sockptr include/linux/sockptr.h:55 [inline] BUG: KASAN: slab-out-of-bounds in nfc_llcp_setsockopt+0x6c2/0x850 net/nfc/llcp_sock.c:255 Read of size 4 at addr ffff88801caa1ec3 by task syz-executor459/5078 CPU: 0 PID: 5078 Comm: syz-executor459 Not tainted 6.8.0-syzkaller-08951-gfe46a7dd189e #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:114 print_address_description mm/kasan/report.c:377 [inline] print_report+0x169/0x550 mm/kasan/report.c:488 kasan_report+0x143/0x180 mm/kasan/report.c:601 copy_from_sockptr_offset include/linux/sockptr.h:49 [inline] copy_from_sockptr include/linux/sockptr.h:55 [inline] nfc_llcp_setsockopt+0x6c2/0x850 net/nfc/llcp_sock.c:255 do_sock_setsockopt+0x3b1/0x720 net/socket.c:2311 __sys_setsockopt+0x1ae/0x250 net/socket.c:2334 __do_sys_setsockopt net/socket.c:2343 [inline] __se_sys_setsockopt net/socket.c:2340 [inline] __x64_sys_setsockopt+0xb5/0xd0 net/socket.c:2340 do_syscall_64+0xfd/0x240 entry_SYSCALL_64_after_hwframe+0x6d/0x75 RIP: 0033:0x7f7fac07fd89 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 91 18 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:00007fff660eb788 EFLAGS: 00000246 ORIG_RAX: 0000000000000036 RAX: ffffffffffffffda RBX: 0000000000000003 RCX: 00007f7fac07fd89 RDX: 0000000000000000 RSI: 0000000000000118 RDI: 0000000000000004 RBP: 0000000000000000 R08: 0000000000000002 R09: 0000000000000000 R10: 0000000020000a80 R11: 0000000000000246 R12: 0000000000000000 R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000	N/A	More Details
CVE-2024-36918	In the Linux kernel, the following vulnerability has been resolved: bpf: Check bloom filter map value size This patch adds a missing check to bloom filter creating, rejecting values above KMALLOC_MAX_SIZE. This brings the bloom map in line with many other map types. The lack of this protection can cause kernel crashes for value sizes that overflow int's. Such a crash was caught by syzkaller. The next patch adds more guard-rails at a lower level.	N/A	More Details
CVE-2024-36917	In the Linux kernel, the following vulnerability has been resolved: block: fix overflow in blk_ioctl_discard() There is no check for overflow of 'start + len' in blk_ioctl_discard(). Hung task occurs if submit an discard ioctl with the following param: start = 0x80000000000ff000, len = 0x8000000000fff000; Add the overflow validation now.	N/A	More Details
CVE-2024-36890	In the Linux kernel, the following vulnerability has been resolved: mm/slab: make __free(kfree) accept error pointers Currently, if an automatically freed allocation is an error pointer that will lead to a crash. An example of this is in wm831x_gpio_dbg_show(). 171 char *label __free(kfree) = gpiochip_dup_line_label(chip, i); 172 if (IS_ERR(label)) { 173 dev_err(wm831x->dev, "Failed to duplicate label\n"); 174 continue; 175 } The auto clean up function should check for error pointers as well, otherwise we're going to keep hitting issues like this.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36919	In the Linux kernel, the following vulnerability has been resolved: scsi: bnx2fc: Remove spin_lock_bh while releasing resources after upload The session resources are used by FW and driver when session is offloaded, once session is uploaded these resources are not used. The lock is not required as these fields won't be used any longer. The offload and upload calls are sequential, hence lock is not required. This will suppress following BUG_ON(): [449.843143] ------------[cut here]------------ [449.848302] kernel BUG at mm/vmalloc.c:2727! [449.853072] invalid opcode: 0000 [#1] PREEMPT SMP PTI [449.858712] CPU: 5 PID: 1996 Comm: kworker/u24:2 Not tainted 5.14.0-118.el9.x86_64 #1 Rebooting. [449.867454] Hardware name: Dell Inc. PowerEdge R730/0WCJNT, BIOS 2.3.4 11/08/2016 [449.876966] Workqueue: fc_rport_eq fc_rport_work [libfc] [449.882910] RIP: 0010:vunmap+0x2e/0x30 [449.887098] Code: 00 65 8b 05 14 a2 f0 4a a9 00 ff ff 00 75 1b 55 48 89 fd e8 34 36 79 00 48 85 ed 74 0b 48 89 ef 31 f6 5d e9 14 fc ff ff 5d c3 <0f> 0b 0f 1f 44 00 00 41 57 41 56 49 89 ce 41 55 49 89 fd 41 54 41 [449.908054] RSP: 0018:ffffb83d878b3d68 EFLAGS: 00010206 [449.913887] RAX: 0000000080000201 RBX: ffff8f4355133550 RCX: 000000000d400005 [449.921843] RDX: 0000000000000001 RSI: 0000000000001000 RDI: ffffb83da53f5000 [449.929808] RBP: ffff8f4ac6675800 R08: ffffb83d878b3d30 R09: 00000000000efbdf [449.937774] R10: 0000000000000003 R11: ffff8f434573e000 R12: 0000000000001000 [449.945736] R13: 0000000000001000 R14: ffffb83da53f5000 R15: ffff8f43d4ea3ae0 [449.953701] FS: 0000000000000000(0000) GS:ffff8f529fc80000(0000) knlGS:0000000000000000 [449.962732] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [449.969138] CR2: 00007f8cf993e150 CR3: 0000000efbe10003 CR4: 00000000003706e0 [449.977102] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [449.985065] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [449.993028] Call Trace: [449.995756] __iommu_dma_free+0x96/0x100 [450.000139] bnx2fc_free_session_resc+0x67/0x240 [bnx2fc] [450.006171] bnx2fc_upload_session+0xce/0x100 [bnx2fc] [450.011910] bnx2fc_rport_event_handler+0x9f/0x240 [bnx2fc] [450.018136] fc_rport_work+0x103/0x5b0 [libfc] [450.023103] process_one_work+0x1e8/0x3c0 [450.027581] worker_thread+0x50/0x3b0 [450.031669] ? rescuer_thread+0x370/0x370 [450.036143] kthread+0x149/0x170 [450.039744] ? set_kthread_struct+0x40/0x40 [450.044411] ret_from_fork+0x22/0x30 [450.048404] Modules linked in: vfat msdos fat xfs nfs_layout_nfsv41_files rpcsec_gss_krb5 auth_rpcgss nfsv4 dns_resolver dm_service_time qedf qed crc8 bnx2fc libfcoe libfc scsi_transport_fc intel_rapl_msr intel_rapl_common x86_pkg_temp_thermal intel_powerclamp dcdbas rapl intel_cstate intel_uncore mei_me pcspkr mei ipmi_ssif lpc_ich ipmi_si fuse zram ext4 mbcache jbd2 loop nfsv3 nfs_acl nfs lockd grace fscache netfs irdma ice sd_mod t10_pi sg ib_uverbs ib_core 8021q garp mrp stp llc mgag200 i2c_algo_bit drm_kms_helper syscopyarea sysfillrect sysimgblt mxm_wmi fb_sys_fops cec crct10dif_pclmul ahci crc32_pclmul bnx2x drm ghash_clmulni_intel libahci rfkill i40e libata megaraid_sas mdio wmi sunrpc lrw dm_crypt dm_round_robin dm_multipath dm_snapshot dm_bufio dm_mirror dm_region_hash dm_log dm_zero dm_mod linear raid10 raid456 async_raid6_recov async_memcpy async_pq async_xor async_tx raid6_pq libcrc32c crc32c_intel raid1 raid0 iscsi_ibft squashfs be2iscsi bnx2i cnic uio cxgb4i cxgb4 tls [450.048497] libcxgbi libcxgb qla4xxx iscsi_boot_sysfs iscsi_tcp libiscsi_tcp libiscsi scsi_transport_iscsi edd ipmi_devintf ipmi_msghandler [450.159753] ---[end trace 712de2c57c64abc8]---	N/A	More Details
CVE-2024-36920	In the Linux kernel, the following vulnerability has been resolved: scsi: mpi3mr: Avoid memcpy field-spanning write WARNING When the "storcli2 show" command is executed for eHBA-9600, mpi3mr driver prints this WARNING message: memcpy: detected field-spanning write (size 128) of single field "bsg_reply_buf->reply_buf" at drivers/scsi/mpi3mr/mpi3mr_app.c:1658 (size 1) WARNING: CPU: 0 PID: 12760 at drivers/scsi/mpi3mr/mpi3mr_app.c:1658 mpi3mr_bsg_request+0x6b12/0x7f10 [mpi3mr] The cause of the WARN is 128 bytes memcpy to the 1 byte size array "__u8 replay_buf[1]" in the struct mpi3mr_bsg_in_reply_buf. The array is intended to be a flexible length array, so the WARN is a false positive. To suppress the WARN, remove the constant number '1' from the array declaration and clarify that it has flexible length. Also, adjust the memory allocation size to match the change.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36921	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mvm: guard against invalid STA ID on removal Guard against invalid station IDs in iwl_mvm_mld_rm_sta_id as that would result in out-of-bounds array accesses. This prevents issues should the driver get into a bad state during error handling.	N/A	More Details
CVE-2024-36922	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: read txq->read_ptr under lock If we read txq->read_ptr without lock, we can read the same value twice, then obtain the lock, and reclaim from there to two different places, but crucially reclaim the same entry twice, resulting in the WARN_ONCE() a little later. Fix that by reading txq->read_ptr under lock.	N/A	More Details
CVE-2024-36923	In the Linux kernel, the following vulnerability has been resolved: fs/9p: fix uninitialized values during inode evict If an iget fails due to not being able to retrieve information from the server then the inode structure is only partially initialized. When the inode gets evicted, references to uninitialized structures (like fscache cookies) were being made. This patch checks for a bad_inode before doing anything other than clearing the inode from the cache. Since the inode is bad, it shouldn't have any state associated with it that needs to be written back (and there really isn't a way to complete those anyways).	N/A	More Details
CVE-2024-36924	In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Release hbalock before calling lpfc_worker_wake_up() lpfc_worker_wake_up() calls the lpfc_work_done() routine, which takes the hbalock. Thus, lpfc_worker_wake_up() should not be called while holding the hbalock to avoid potential deadlock.	N/A	More Details
CVE-2024-36927	In the Linux kernel, the following vulnerability has been resolved: ipv4: Fix uninit-value access in __ip_make_skb() KMSAN reported uninit-value access in __ip_make_skb() [1]. __ip_make_skb() tests HDRINCL to know if the skb has icmphdr. However, HDRINCL can cause a race condition. If calling setsockopt(2) with IP_HDRINCL changes HDRINCL while __ip_make_skb() is running, the function will access icmphdr in the skb even if it is not included. This causes the issue reported by KMSAN. Check FLOWI_FLAG_KNOWN_NH on fl4->flowi4_flags instead of testing HDRINCL on the socket. Also, fl4->fl4_icmp_type and fl4->fl4_icmp_code are not initialized. These are union in struct flowi4 and are implicitly initialized by flowi4_init_output(), but we should not rely on specific union layout. Initialize these explicitly in raw_sendmsg(). [1] BUG: KMSAN: uninit-value in __ip_make_skb+0x2b74/0x2d20 net/ipv4/ip_output.c:1481 __ip_make_skb+0x2b74/0x2d20 net/ipv4/ip_output.c:1481 ip_finish_skb include/net/ip.h:243 [inline] ip_push_pending_frames+0x4c/0x5c0 net/ipv4/ip_output.c:1508 raw_sendmsg+0x2381/0x2690 net/ipv4/raw.c:654 inet_sendmsg+0x27b/0x2a0 net/ipv4/af_inet.c:851 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x274/0x3c0 net/socket.c:745 __sys_sendto+0x62c/0x7b0 net/socket.c:2191 __do_sys_sendto net/socket.c:2203 [inline] __se_sys_sendto net/socket.c:2199 [inline] __x64_sys_sendto+0x130/0x200 net/socket.c:2199 do_syscall_64+0xd8/0x1f0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x6d/0x75 Uninit was created at: slab_post_alloc_hook mm/slub.c:3804 [inline] slab_alloc_node mm/slub.c:3845 [inline] kmem_cache_alloc_node+0x5f6/0xc50 mm/slub.c:3888 kmalloc_reserve+0x13c/0x4a0 net/core/skbuff.c:577 __alloc_skb+0x35a/0x7c0 net/core/skbuff.c:668 alloc_skb include/linux/skbuff.h:1318 [inline] __ip_append_data+0x49ab/0x68c0 net/ipv4/ip_output.c:1128 ip_append_data+0x1e7/0x260 net/ipv4/ip_output.c:1365 raw_sendmsg+0x22b1/0x2690 net/ipv4/raw.c:648 inet_sendmsg+0x27b/0x2a0 net/ipv4/af_inet.c:851 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x274/0x3c0 net/socket.c:745 __sys_sendto+0x62c/0x7b0 net/socket.c:2191 __do_sys_sendto net/socket.c:2203 [inline] __se_sys_sendto net/socket.c:2199 [inline] __x64_sys_sendto+0x130/0x200 net/socket.c:2199 do_syscall_64+0xd8/0x1f0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x6d/0x75 CPU: 1 PID: 15709 Comm: syz-executor.7 Not tainted 6.8.0-11567-gb3603fcb79b1 #25 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-1.fc39 04/01/2014	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36929	In the Linux kernel, the following vulnerability has been resolved: net: core: reject skb_copy(_expand) for fraglist GSO skbs SKB_GSO_FRAGLIST skbs must not be linearized, otherwise they become invalid. Return NULL if such an skb is passed to skb_copy or skb_copy_expand, in order to prevent a crash on a potential later call to skb_gso_segment.	N/A	More Details
CVE-2024-36931	In the Linux kernel, the following vulnerability has been resolved: s390/cio: Ensure the copied buf is NUL terminated Currently, we allocate a lbuf-sized kernel buffer and copy lbuf from userspace to that buffer. Later, we use scanf on this buffer but we don't ensure that the string is terminated inside the buffer, this can lead to OOB read when using scanf. Fix this issue by using memdup_user_nul instead.	N/A	More Details
CVE-2024-36933	In the Linux kernel, the following vulnerability has been resolved: nsh: Restore skb->{protocol,data,mac_header} for outer header in nsh_gso_segment(). syzbot triggered various splats (see [0] and links) by a crafted GSO packet of VIRTIO_NET_HDR_GSO_UDP layering the following protocols: ETH_P_8021AD + ETH_P_NSH + ETH_P_IPV6 + IPPROTO_UDP NSH can encapsulate IPv4, IPv6, Ethernet, NSH, and MPLS. As the inner protocol can be Ethernet, NSH GSO handler, nsh_gso_segment(), calls skb_mac_gso_segment() to invoke inner protocol GSO handlers. nsh_gso_segment() does the following for the original skb before calling skb_mac_gso_segment() 1. reset skb->network_header 2. save the original skb->{mac_heaeder,mac_len} in a local variable 3. pull the NSH header 4. resets skb->mac_header 5. set up skb->mac_len and skb->protocol for the inner protocol. and does the following for the segmented skb 6. set ntohs(ETH_P_NSH) to skb->protocol 7. push the NSH header 8. restore skb->mac_header 9. set skb->mac_header + mac_len to skb->network_header 10. restore skb->mac_len There are two problems in 6-7 and 8-9. (a) After 6 & 7, skb->data points to the NSH header, so the outer header (ETH_P_8021AD in this case) is stripped when skb is sent out of netdev. Also, if NSH is encapsulated by NSH + Ethernet (so NSH-Ethernet-NSH), skb_pull() in the first nsh_gso_segment() will make skb->data point to the middle of the outer NSH or Ethernet header because the Ethernet header is not pulled by the second nsh_gso_segment(). (b) While restoring skb->{mac_header,network_header} in 8 & 9, nsh_gso_segment() does not assume that the data in the linear buffer is shifted. However, udp6_ufo_fragment() could shift the data and change skb->mac_header accordingly as demonstrated by syzbot. If this happens, even the restored skb->mac_header points to the middle of the outer header. It seems nsh_gso_segment() has never worked with outer headers so far. At the end of nsh_gso_segment(), the outer header must be restored for the segmented skb, instead of the NSH header. To do that, let's calculate the outer header position relatively from the inner header and set skb->{data,mac_header,protocol} properly. [0]: BUG: KMSAN: uninit-value in ipvlan_process_outbound drivers/net/ipvlan/ipvlan_core.c:524 [inline] BUG: KMSAN: uninit-value in ipvlan_xmit_mode_l3 drivers/net/ipvlan/ipvlan_core.c:602 [inline] BUG: KMSAN: uninit-value in ipvlan_queue_xmit+0xf44/0x16b0 drivers/net/ipvlan/ipvlan_core.c:668 ipvlan_process_outbound drivers/net/ipvlan/ipvlan_core.c:524 [inline] ipvlan_xmit_mode_l3 drivers/net/ipvlan/ipvlan_core.c:602 [inline] ipvlan_queue_xmit+0xf44/0x16b0 drivers/net/ipvlan/ipvlan_core.c:668 ipvlan_start_xmit+0x5c/0x1a0 drivers/net/ipvlan/ipvlan_main.c:222 __netdev_start_xmit include/linux/netdevice.h:4989 [inline] netdev_start_xmit include/linux/netdevice.h:5003 [inline] xmit_one net/core/dev.c:3547 [inline] dev_hard_start_xmit+0x244/0xa10 net/core/dev.c:3563 __dev_queue_xmit+0x33ed/0x51c0 net/core/dev.c:4351 dev_queue_xmit include/linux/netdevice.h:3171 [inline] packet_xmit+0x9c/0x6b0 net/packet/af_packet.c:276 packet_snd net/packet/af_packet.c:3081 [inline] packet_sendmsg+0x8aef/0x9f10 net/packet/af_packet.c:3113 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg net/socket.c:745 [inline] __sys_sendto+0x735/0xa10 net/socket.c:2191 __do_sys_sendto net/socket.c:2203 [inline] __se_sys_sendto net/socket.c:2199 [inline] __x64_sys_sendto+0x125/0x1c0 net/socket.c:2199 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b Uninit was created at: slab_post_alloc_hook mm/slub.c:3819 [inline] slab_alloc_node mm/slub.c:3860 [inline] __do_kmalloc_node mm/slub.c:3980 [inline] __kmalloc_node_track_caller+0x705/0x1000 mm/slub.c:4001 kmalloc_reserve+0x249/0x4a0 net/core/skbuff.c:582 __ ---truncated---	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36934	In the Linux kernel, the following vulnerability has been resolved: bna: ensure the copied buf is NUL terminated Currently, we allocate a nbytes-sized kernel buffer and copy nbytes from userspace to that buffer. Later, we use sscanf on this buffer but we don't ensure that the string is terminated inside the buffer, this can lead to OOB read when using sscanf. Fix this issue by using memdup_user_nul instead of memdup_user.	N/A	More Details
CVE-2024-36935	In the Linux kernel, the following vulnerability has been resolved: ice: ensure the copied buf is NUL terminated Currently, we allocate a count-sized kernel buffer and copy count bytes from userspace to that buffer. Later, we use sscanf on this buffer but we don't ensure that the string is terminated inside the buffer, this can lead to OOB read when using sscanf. Fix this issue by using memdup_user_nul instead of memdup_user.	N/A	More Details
CVE-2024-36936	In the Linux kernel, the following vulnerability has been resolved: efi/unaccepted: touch soft lockup during memory accept Commit 50e782a86c98 ("efi/unaccepted: Fix soft lockups caused by parallel memory acceptance") has released the spinlock so other CPUs can do memory acceptance in parallel and not triggers softlockup on other CPUs. However the softlock up was intermittent shown up if the memory of the TD guest is large, and the timeout of softlockup is set to 1 second: RIP: 0010:_raw_spin_unlock_irqrestore Call Trace: ? __hrtimer_run_queues <IRQ> ? hrtimer_interrupt ? watchdog_timer_fn ? __sysvec_apic_timer_interrupt ? __pfx_watchdog_timer_fn ? sysvec_apic_timer_interrupt </IRQ> ? __hrtimer_run_queues <TASK> ? hrtimer_interrupt ? asm_sysvec_apic_timer_interrupt ? _raw_spin_unlock_irqrestore ? __sysvec_apic_timer_interrupt ? sysvec_apic_timer_interrupt accept_memory try_to_accept_memory do_huge_pmd_anonymous_page get_page_from_freelist __handle_mm_fault __alloc_pages __folio_alloc ? __tdx_hypercall handle_mm_fault vma_alloc_folio do_user_addr_fault do_huge_pmd_anonymous_page exc_page_fault ? __do_huge_pmd_anonymous_page asm_exc_page_fault __handle_mm_fault When the local irq is enabled at the end of accept_memory(), the softlockup detects that the watchdog on single CPU has not been fed for a while. That is to say, even other CPUs will not be blocked by spinlock, the current CPU might be stunk with local irq disabled for a while, which hurts not only nmi watchdog but also softlockup. Chao Gao pointed out that the memory accept could be time costly and there was similar report before. Thus to avoid any softlocup detection during this stage, give the softlockup a flag to skip the timeout check at the end of accept_memory(), by invoking touch_softlockup_watchdog().	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36892	In the Linux kernel, the following vulnerability has been resolved: mm/slub: avoid zeroing outside-object freepointer for single free Commit 284f17ac13fe ("mm/slub: handle bulk and single object freeing separately") splits single and bulk object freeing in two functions slab_free() and slab_free_bulk() which leads slab_free() to call slab_free_hook() directly instead of slab_free_freelist_hook(). If `init_on_free` is set, slab_free_hook() zeroes the object. Afterward, if `slub_debug=F` and `CONFIG_SLAB_FREELIST_HARDENED` are set, the do_slab_free() slowpath executes freelist consistency checks and try to decode a zeroed freepointer which leads to a "Freepointer corrupt" detection in check_object(). During bulk free, slab_free_freelist_hook() isn't affected as it always sets it objects freepointer using set_freepointer() to maintain its reconstructed freelist after `init_on_free`. For single free, object's freepointer thus needs to be avoided when stored outside the object if `init_on_free` is set. The freepointer left as is, check_object() may later detect an invalid pointer value due to objects overflow. To reproduce, set `slub_debug=FU init_on_free=1 log_level=7` on the command line of a kernel build with `CONFIG_SLAB_FREELIST_HARDENED=y`. dmesg sample log: [10.708715] ========== [10.710323] BUG kmalloc-rnd-05-32 (Tainted: G B T): Freepointer corrupt [10.712695] ---------- [10.712695] [10.712695] Slab 0xffffd8bdc400d580 objects=32 used=4 fp=0xffff9d9a80356f80 flags=0x200000000000a00(workingsetlslablnode=0lzone=2) [10.716698] Object 0xffff9d9a80356600 @offset=1536 fp=0x7ee4f480ce0ecd7c [10.716698] [10.716698] Bytes b4 ffff9d9a803565f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... [10.720703] Object ffff9d9a80356600: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... [10.720703] Object ffff9d9a80356610: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... [10.724696] Padding ffff9d9a8035666c: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... [10.724696] Padding ffff9d9a8035667c: 00 00 00 00 .... [10.724696] FIX kmalloc-rnd-05-32: Object at 0xffff9d9a80356600 not freed	N/A	More Details
CVE-2024-36885	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36889	In the Linux kernel, the following vulnerability has been resolved: mptcp: ensure snd_nxt is properly initialized on connect Christoph reported a splat hinting at a corrupted snd_una: WARNING: CPU: 1 PID: 38 at net/mptcp/protocol.c:1005 __mptcp_clean_una+0x4b3/0x620 net/mptcp/protocol.c:1005 Modules linked in: CPU: 1 PID: 38 Comm: kworker/1:1 Not tainted 6.9.0-rc1-gbbeac67456c9 #59 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.11.0-2.el7 04/01/2014 Workqueue: events mptcp_worker RIP: 0010:__mptcp_clean_una+0x4b3/0x620 net/mptcp/protocol.c:1005 Code: be 06 01 00 00 bf 06 01 00 00 e8 a8 12 e7 fe e9 00 fe ff ff e8 8e 1a e7 fe 0f b7 ab 3e 02 00 00 e9 d3 fd ff ff e8 7d 1a e7 fe <0f> 0b 4c 8b bb e0 05 00 00 e9 74 fc ff ff e8 6a 1a e7 fe 0f 0b e9 RSP: 0018:ffffc9000013fd48 EFLAGS: 00010293 RAX: 0000000000000000 RBX: ffff8881029bd280 RCX: ffffffff82382fe4 RDX: ffff8881003cbd00 RSI: ffffffff823833c3 RDI: 0000000000000001 RBP: 0000000000000000 R08: 0000000000000001 R09: 0000000000000000 R10: 0000000000000000 R11: fefefefefefefeff R12: ffff888138ba8000 R13: 0000000000000106 R14: ffff8881029bd908 R15: ffff888126560000 FS: 0000000000000000(0000) GS:ffff88813bd00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f604a5dae38 CR3: 0000000101dac002 CR4: 0000000000170ef0 Call Trace: <TASK> __mptcp_clean_una_wakeup net/mptcp/protocol.c:1055 [inline] mptcp_clean_una_wakeup net/mptcp/protocol.c:1062 [inline] __mptcp_retrans+0x7f/0x7e0 net/mptcp/protocol.c:2615 mptcp_worker+0x434/0x740 net/mptcp/protocol.c:2767 process_one_work+0x1e0/0x560 kernel/workqueue.c:3254 process_scheduled_works kernel/workqueue.c:3335 [inline] worker_thread+0x3c7/0x640 kernel/workqueue.c:3416 kthread+0x121/0x170 kernel/kthread.c:388 ret_from_fork+0x44/0x50 arch/x86/kernel/process.c:147 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:243 </TASK> When fallback to TCP happens early on a client socket, snd_nxt is not yet initialized and any incoming ack will copy such value into snd_una. If the mptcp worker (dumbly) tries mptcp-level re-injection after such ack, that would unconditionally trigger a send buffer cleanup using 'bad' snd_una values. We could easily disable re-injection for fallback sockets, but such dumb behavior already helped catching a few subtle issues and a very low to zero impact in practice. Instead address the issue always initializing snd_nxt (and write_seq, for consistency) at connect time.	N/A	More Details
CVE-2024-36887	In the Linux kernel, the following vulnerability has been resolved: e1000e: change usleep_range to udelay in PHY mdic access This is a partial revert of commit 6dbdd4de0362 ("e1000e: Workaround for sporadic MDI error on Meteor Lake systems"). The referenced commit used usleep_range inside the PHY access routines, which are sometimes called from an atomic context. This can lead to a kernel panic in some scenarios, such as cable disconnection and reconnection on vPro systems. Solve this by changing the usleep_range calls back to udelay.	N/A	More Details
CVE-2024-3937	The Playlist for Youtube WordPress plugin through 1.32 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	N/A	More Details
CVE-2024-36014	In the Linux kernel, the following vulnerability has been resolved: drm/arm/malidp: fix a possible null pointer dereference In malidp_mw_connector_reset, new memory is allocated with kzalloc, but no check is performed. In order to prevent null pointer dereferencing, ensure that mw_state is checked before calling __drm_atomic_helper_connector_reset.	N/A	More Details
CVE-2024-36015	In the Linux kernel, the following vulnerability has been resolved: ppdev: Add an error check in register_device In register_device, the return value of ida_simple_get is unchecked, in witch ida_simple_get will use an invalid index value. To address this issue, index should be checked after ida_simple_get. When the index value is abnormal, a warning message should be printed, the port should be dropped, and the value should be recorded.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52881	In the Linux kernel, the following vulnerability has been resolved: tcp: do not accept ACK of bytes we never sent This patch is based on a detailed report and ideas from Yepeng Pan and Christian Rossow. ACK seq validation is currently following RFC 5961 5.2 guidelines: The ACK value is considered acceptable only if it is in the range of ((SND.UNA - MAX.SND.WND) <= SEG.ACK <= SND.NXT). All incoming segments whose ACK value doesn't satisfy the above condition MUST be discarded and an ACK sent back. It needs to be noted that RFC 793 on page 72 (fifth check) says: "If the ACK is a duplicate (SEG.ACK < SND.UNA), it can be ignored. If the ACK acknowledges something not yet sent (SEG.ACK > SND.NXT) then send an ACK, drop the segment, and return". The "ignored" above implies that the processing of the incoming data segment continues, which means the ACK value is treated as acceptable. This mitigation makes the ACK check more stringent since any ACK < SND.UNA wouldn't be accepted, instead only ACKs that are in the range ((SND.UNA - MAX.SND.WND) <= SEG.ACK <= SND.NXT) get through. This can be refined for new (and possibly spoofed) flows, by not accepting ACK for bytes that were never sent. This greatly improves TCP security at a little cost. I added a Fixes: tag to make sure this patch will reach stable trees, even if the 'blamed' patch was adhering to the RFC. tp->bytes_acked was added in linux-4.2 Following packetdrill test (courtesy of Yepeng Pan) shows the issue at hand: 0 socket(..., SOCK_STREAM, IPPROTO_TCP) = 3 +0 setsockopt(3, SOL_SOCKET, SO_REUSEADDR, [1], 4) = 0 +0 bind(3, ..., ...) = 0 +0 listen(3, 1024) = 0 // ---------- Handshake ---------- // // when window scale is set to 14 the window size can be extended to // 65535 * (2^14) = 1073725440. Linux would accept an ACK packet // with ack number in (Server_ISN+1-1073725440. Server_ISN+1) // ,though this ack number acknowledges some data never // sent by the server. +0 < S 0:0(0) win 65535 <mss 1400,nop,wscale 14> +0 > S. 0:0(0) ack 1 <...> +0 < . 1:1(0) ack 1 win 65535 +0 accept(3, ..., ...) = 4 // For the established connection, we send an ACK packet, // the ack packet uses ack number 1 - 1073725300 + 2^32, // where 2^32 is used to wrap around. // Note: we used 1073725300 instead of 1073725440 to avoid possible // edge cases. // 1 - 1073725300 + 2^32 = 3221241997 // Oops, old kernels happily accept this packet. +0 < . 1:1001(1000) ack 3221241997 win 65535 // After the kernel fix the following will be replaced by a challenge ACK, // and prior malicious frame would be dropped. +0 > . 1:1(0) ack 1001	N/A	More Details
CVE-2024-25976	When LDAP authentication is activated in the configuration it is possible to obtain reflected XSS execution by creating a custom URL that the victim only needs to open in order to execute arbitrary JavaScript code in the victim's browser. This is due to a fault in the file login.php where the content of "$_SERVER['PHP_SELF']" is reflected into the HTML of the website. Hence the attacker does not need a valid account in order to exploit this issue.	N/A	More Details
CVE-2024-35284	A vulnerability in the legacy chat component of Mitel MiContact Center Business through 10.0.0.4 could allow an unauthenticated attacker to conduct a reflected cross-site scripting (XSS) attack due to insufficient input validation.	N/A	More Details
CVE-2024-36017	In the Linux kernel, the following vulnerability has been resolved: rtnetlink: Correct nested IFLA_VF_VLAN_LIST attribute validation Each attribute inside a nested IFLA_VF_VLAN_LIST is assumed to be a struct ifla_vf_vlan_info so the size of such attribute needs to be at least of sizeof(struct ifla_vf_vlan_info) which is 14 bytes. The current size validation in do_setvfinfo is against NLA_HDRLEN (4 bytes) which is less than sizeof(struct ifla_vf_vlan_info) so this validation is not enough and a too small attribute might be cast to a struct ifla_vf_vlan_info, this might result in an out of bands read access when accessing the saved (casted) entry in ivvl.	N/A	More Details
CVE-2024-3584	qdrant/qdrant version 1.9.0-dev is vulnerable to path traversal due to improper input validation in the `/collections/{name}/snapshots/upload` endpoint. By manipulating the `name` parameter through URL encoding, an attacker can upload a file to an arbitrary location on the system, such as `/root/poc.txt`. This vulnerability allows for the writing and overwriting of arbitrary files on the server, potentially leading to a full takeover of the system. The issue is fixed in version 1.9.0.	N/A	More Details
CVE-2024-35504	A cross-site scripting (XSS) vulnerability in the login page of FineSoft v8.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the URL:errorname parameter after a failed login attempt.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36018	In the Linux kernel, the following vulnerability has been resolved: nouveau/uvmm: fix addr/range calcs for remap operations dEQP-VK.sparse_resources.image_rebind.2d_array.r64i.128_128_8 was causing a remap operation like the below. op_remap: prev: 0000003fffed0000 00000000000f0000 00000000a5abd18a 0000000000000000 op_remap: next: op_remap: unmap: 0000003fffed0000 0000000000100000 0 op_map: map: 0000003ffffc0000 0000000000010000 000000005b1ba33c 00000000000e0000 This was resulting in an unmap operation from 0x3fffed0000+0xf0000, 0x100000 which was corrupting the pagetables and oopsing the kernel. Fixes the prev + unmap range calcs to use start/end and map back to addr/range.	N/A	More Details
CVE-2024-36019	In the Linux kernel, the following vulnerability has been resolved: regmap: maple: Fix cache corruption in regcache_maple_drop() When keeping the upper end of a cache block entry, the entry[] array must be indexed by the offset from the base register of the block, i.e. max - mas.index. The code was indexing entry[] by only the register address, leading to an out-of-bounds access that copied some part of the kernel memory over the cache contents. This bug was not detected by the regmap KUnit test because it only tests with a block of registers starting at 0, so mas.index == 0.	N/A	More Details
CVE-2024-36020	In the Linux kernel, the following vulnerability has been resolved: i40e: fix vf may be used uninitialized in this function warning To fix the regression introduced by commit 52424f974bc5, which causes servers hang in very hard to reproduce conditions with resets races. Using two sources for the information is the root cause. In this function before the fix bumping v didn't mean bumping vf pointer. But the code used this variables interchangeably, so stale vf could point to different/not intended vf. Remove redundant "v" variable and iterate via single VF pointer across whole function instead to guarantee VF pointer validity.	N/A	More Details
CVE-2024-36021	In the Linux kernel, the following vulnerability has been resolved: net: hns3: fix kernel crash when devlink reload during pf initialization The devlink reload process will access the hardware resources, but the register operation is done before the hardware is initialized. So, processing the devlink reload during initialization may lead to kernel crash. This patch fixes this by taking devl_lock during initialization.	N/A	More Details
CVE-2024-36022	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Init zone device and drm client after mode-1 reset on reload In passthrough environment, when amdgpu is reloaded after unload, mode-1 is triggered after initializing the necessary IPs, That init does not include KFD, and KFD init waits until the reset is completed. KFD init is called in the reset handler, but in this case, the zone device and drm client is not initialized, causing app to create kernel panic. v2: Removing the init KFD condition from amdgpu_amdkfd_drm_client_create. As the previous version has the potential of creating DRM client twice. v3: v2 patch results in SDMA engine hung as DRM open causes VM clear to SDMA before SDMA init. Adding the condition to in drm client creation, on top of v1, to guard against drm client creation call multiple times.	N/A	More Details
CVE-2024-36024	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Disable idle reallow as part of command/gpint execution [Why] Workaroud for a race condition where DMCUB is in the process of committing to IPS1 during the handshake causing us to miss the transition into IPS2 and touch the INBOX1 RPTR causing a HW hang. [How] Disable the reallow to ensure that we have enough of a gap between entry and exit and we're not seeing back-to-back wake_and_executes.	N/A	More Details
CVE-2024-36025	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Fix off by one in qla_edif_app_getstats() The app_reply->elem[] array is allocated earlier in this function and it has app_req.num_ports elements. Thus this > comparison needs to be >= to prevent memory corruption.	N/A	More Details
CVE-2024-36026	In the Linux kernel, the following vulnerability has been resolved: drm/amd/pm: fixes a random hang in S4 for SMU v13.0.4/11 While doing multiple S4 stress tests, GC/RLC/PMFW get into an invalid state resulting into hard hangs. Adding a GFX reset as workaround just before sending the MP1_UNLOAD message avoids this failure.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3924	A code injection vulnerability exists in the huggingface/text-generation-inference repository, specifically within the `autodocs.yml` workflow file. The vulnerability arises from the insecure handling of the `github.head_ref` user input, which is used to dynamically construct a command for installing a software package. An attacker can exploit this by forking the repository, creating a branch with a malicious payload as the name, and then opening a pull request to the base repository. Successful exploitation could lead to arbitrary code execution within the context of the GitHub Actions runner. This issue affects versions up to and including v2.0.0 and was fixed in version 2.0.0.	N/A	More Details
CVE-2024-4330	A path traversal vulnerability was identified in the parisneo/lollms-webui repository, specifically within version 9.6. The vulnerability arises due to improper handling of user-supplied input in the 'list_personalities' endpoint. By crafting a malicious HTTP request, an attacker can traverse the directory structure and view the contents of any folder, albeit limited to subfolder names only. This issue was demonstrated via a specific HTTP request that manipulated the 'category' parameter to access arbitrary directories. The vulnerability is present in the code located at the 'endpoints/lollms_advanced.py' file.	N/A	More Details
CVE-2023-52882	In the Linux kernel, the following vulnerability has been resolved: clk: sunxi-ng: h6: Reparent CPUX during PLL CPUX rate change While PLL CPUX clock rate change when CPU is running from it works in vast majority of cases, now and then it causes instability. This leads to system crashes and other undefined behaviour. After a lot of testing (30+ hours) while also doing a lot of frequency switches, we can't observe any instability issues anymore when doing reparenting to stable clock like 24 MHz oscillator.	N/A	More Details
CVE-2024-32029	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2024-36027	In the Linux kernel, the following vulnerability has been resolved: btrfs: zoned: do not flag ZEROOUT on non-dirty extent buffer Btrfs clears the content of an extent buffer marked as EXTENT_BUFFER_ZONED_ZEROOUT before the bio submission. This mechanism is introduced to prevent a write hole of an extent buffer, which is once allocated, marked dirty, but turns out unnecessary and cleaned up within one transaction operation. Currently, btrfs_clear_buffer_dirty() marks the extent buffer as EXTENT_BUFFER_ZONED_ZEROOUT, and skips the entry function. If this call happens while the buffer is under IO (with the WRITEBACK flag set, without the DIRTY flag), we can add the ZEROOUT flag and clear the buffer's content just before a bio submission. As a result: 1) it can lead to adding faulty delayed reference item which leads to a FS corrupted (EUCLEAN) error, and 2) it writes out cleared tree node on disk The former issue is previously discussed in [1]. The corruption happens when it runs a delayed reference update. So, on-disk data is safe. [1] https://lore.kernel.org/linux-btrfs/3f4f2a0ff1a6c818050434288925bdcf3cd719e5.1709124777.git.naohiro.aota@wdc.com/ The latter one can reach on-disk data. But, as that node is already processed by btrfs_clear_buffer_dirty(), that will be invalidated in the next transaction commit anyway. So, the chance of hitting the corruption is relatively small. Anyway, we should skip flagging ZEROOUT on a non-DIRTY extent buffer, to keep the content under IO intact.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36028	In the Linux kernel, the following vulnerability has been resolved: mm/hugetlb: fix DEBUG_LOCKS_WARN_ON(1) when dissolve_free_hugetlb_folio() When I did memory failure tests recently, below warning occurs: DEBUG_LOCKS_WARN_ON(1) WARNING: CPU: 8 PID: 1011 at kernel/locking/lockdep.c:232 __lock_acquire+0xccb/0x1ca0 Modules linked in: mce_inject hwpoison_inject CPU: 8 PID: 1011 Comm: bash Kdump: loaded Not tainted 6.9.0-rc3-next-20240410-00012-gdb69f219f4be #3 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.14.0-0-g155821a1990b-prebuilt.qemu.org 04/01/2014 RIP: 0010:__lock_acquire+0xccb/0x1ca0 RSP: 0018:ffffa7a1c7fe3bd0 EFLAGS: 00000082 RAX: 0000000000000000 RBX: eb851eb853975fcf RCX: ffffa1ce5fc1c9c8 RDX: 00000000ffffffd8 RSI: 0000000000000027 RDI: ffffa1ce5fc1c9c0 RBP: ffffa1c6865d3280 R08: fffffffb0f570a8 R09: 0000000000009ffb R10: 0000000000000286 R11: fffffffb0f2ad50 R12: ffffa1c6865d3d10 R13: ffffa1c6865d3c70 R14: 0000000000000000 R15: 0000000000000004 FS: 00007ff9f32aa740(0000) GS:ffffa1ce5fc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007ff9f3134ba0 CR3: 00000008484e4000 CR4: 00000000000006f0 Call Trace: <TASK> lock_acquire+0xbe/0x2d0 _raw_spin_lock_irqsave+0x3a/0x60 hugepage_subpool_put_pages.part.0+0xe/0xc0 free_huge_folio+0x253/0x3f0 dissolve_free_huge_page+0x147/0x210 __page_handle_poison+0x9/0x70 memory_failure+0x4e6/0x8c0 hard_offline_page_store+0x55/0xa0 kernfs_fop_write_iter+0x12c/0x1d0 vfs_write+0x380/0x540 ksys_write+0x64/0xe0 do_syscall_64+0xbc/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7ff9f3114887 RSP: 002b:00007ffecbacb458 EFLAGS: 00000246 ORIG_RAX: 0000000000000001 RAX: ffffffffffffffda RBX: 000000000000000c RCX: 00007ff9f3114887 RDX: 000000000000000c RSI: 0000564494164e10 RDI: 0000000000000001 RBP: 0000564494164e10 R08: 00007ff9f31d1460 R09: 000000007fffffff R10: 0000000000000000 R11: 0000000000000246 R12: 000000000000000c R13: 00007ff9f321b780 R14: 00007ff9f3217600 R15: 00007ff9f3216a00 </TASK> Kernel panic - not syncing: kernel: panic_on_warn set ... CPU: 8 PID: 1011 Comm: bash Kdump: loaded Not tainted 6.9.0-rc3-next-20240410-00012-gdb69f219f4be #3 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.14.0-0-g155821a1990b-prebuilt.qemu.org 04/01/2014 Call Trace: <TASK> panic+0x326/0x350 check_panic_on_warn+0x4f/0x50 __warn+0x98/0x190 report_bug+0x18e/0x1a0 handle_bug+0x3d/0x70 exc_invalid_op+0x18/0x70 asm_exc_invalid_op+0x1a/0x20 RIP: 0010:__lock_acquire+0xccb/0x1ca0 RSP: 0018:ffffa7a1c7fe3bd0 EFLAGS: 00000082 RAX: 0000000000000000 RBX: eb851eb853975fcf RCX: ffffa1ce5fc1c9c8 RDX: 00000000ffffffd8 RSI: 0000000000000027 RDI: ffffa1ce5fc1c9c0 RBP: ffffa1c6865d3280 R08: fffffffb0f570a8 R09: 0000000000009ffb R10: 0000000000000286 R11: fffffffb0f2ad50 R12: ffffa1c6865d3d10 R13: ffffa1c6865d3c70 R14: 0000000000000000 R15: 0000000000000004 lock_acquire+0xbe/0x2d0 _raw_spin_lock_irqsave+0x3a/0x60 hugepage_subpool_put_pages.part.0+0xe/0xc0 free_huge_folio+0x253/0x3f0 dissolve_free_huge_page+0x147/0x210 __page_handle_poison+0x9/0x70 memory_failure+0x4e6/0x8c0 hard_offline_page_store+0x55/0xa0 kernfs_fop_write_iter+0x12c/0x1d0 vfs_write+0x380/0x540 ksys_write+0x64/0xe0 do_syscall_64+0xbc/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7ff9f3114887 RSP: 002b:00007ffecbacb458 EFLAGS: 00000246 ORIG_RAX: 0000000000000001 RAX: ffffffffffffffda RBX: 000000000000000c RCX: 00007ff9f3114887 RDX: 000000000000000c RSI: 0000564494164e10 RDI: 0000000000000001 RBP: 0000564494164e10 R08: 00007ff9f31d1460 R09: 000000007fffffff R10: 0000000000000000 R11: 0000000000000246 R12: 000000000000000c R13: 00007ff9f321b780 R14: 00007ff9f3217600 R15: 00007ff9f3216a00 </TASK> After git bisecting and digging into the code, I believe the root cause is that _deferred_list field of folio is unioned with _hugetlb_subpool field. In __update_and_free_hugetlb_folio(), folio->_deferred_ ---truncated---	N/A	More Details
CVE-2024-36029	In the Linux kernel, the following vulnerability has been resolved: mmc: sdhci-msm: pervent access to suspended controller Generic sdhci code registers LED device and uses host->runtime_suspended flag to protect access to it. The sdhci-msm driver doesn't set this flag, which causes a crash when LED is accessed while controller is runtime suspended. Fix this by setting the flag correctly.	N/A	More Details
CVE-2024-36033	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: qca: fix info leak when fetching board id Add the missing sanity check when fetching the board id to avoid leaking slab data when later requesting the firmware.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36880	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: qca: add missing firmware sanity checks Add the missing sanity checks when parsing the firmware files before downloading them to avoid accessing and corrupting memory beyond the vmalloced buffer.	N/A	More Details
CVE-2024-36882	In the Linux kernel, the following vulnerability has been resolved: mm: use memalloc_nofs_save() in page_cache_ra_order() See commit f2c817bed58d ("mm: use memalloc_nofs_save in readahead path"), ensure that page_cache_ra_order() do not attempt to reclaim file-backed pages too, or it leads to a deadlock, found issue when test ext4 large folio. INFO: task DataXceiver for:7494 blocked for more than 120 seconds. "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message. task:DataXceiver for state:D stack:0 pid:7494 ppid:1 flags:0x00000200 Call trace: __switch_to+0x14c/0x240 __schedule+0x82c/0xdd0 schedule+0x58/0xf0 io_schedule+0x24/0xa0 __folio_lock+0x130/0x300 migrate_pages_batch+0x378/0x918 migrate_pages+0x350/0x700 compact_zone+0x63c/0xb38 compact_zone_order+0xc0/0x118 try_to_compact_pages+0xb0/0x280 __alloc_pages_direct_compact+0x98/0x248 __alloc_pages+0x510/0x1110 alloc_pages+0x9c/0x130 folio_alloc+0x20/0x78 filemap_alloc_folio+0x8c/0x1b0 page_cache_ra_order+0x174/0x308 ondemand_readahead+0x1c8/0x2b8 page_cache_async_ra+0x68/0xb8 filemap_readahead.isra.0+0x64/0xa8 filemap_get_pages+0x3fc/0x5b0 filemap_splice_read+0xf4/0x280 ext4_file_splice_read+0x2c/0x48 [ext4] vfs_splice_read.part.0+0xa8/0x118 splice_direct_to_actor+0xbc/0x288 do_splice_direct+0x9c/0x108 do_sendfile+0x328/0x468 __arm64_sys_sendfile64+0x8c/0x148 invoke_syscall+0x4c/0x118 el0_svc_common.constprop.0+0xc8/0xf0 do_el0_svc+0x24/0x38 el0_svc+0x4c/0x1f8 el0t_64_sync_handler+0xc0/0xc8 el0t_64_sync+0x188/0x190	N/A	More Details
CVE-2024-36883	In the Linux kernel, the following vulnerability has been resolved: net: fix out-of-bounds access in ops_init net_alloc_generic is called by net_alloc, which is called without any locking. It reads max_gen_ptrs, which is changed under pernet_ops_rwsem. It is read twice, first to allocate an array, then to set s.len, which is later used to limit the bounds of the array access. It is possible that the array is allocated and another thread is registering a new pernet ops, increments max_gen_ptrs, which is then used to set s.len with a larger than allocated length for the variable array. Fix it by reading max_gen_ptrs only once in net_alloc_generic. If max_gen_ptrs is later incremented, it will be caught in net_assign_generic.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36939	In the Linux kernel, the following vulnerability has been resolved: nfs: Handle error of rpc_proc_register() in nfs_net_init(). syzkaller reported a warning [0] triggered while destroying immature netns. rpc_proc_register() was called in init_nfs_fs(), but its error has been ignored since at least the initial commit 1da177e4c3f4 ("Linux-2.6.12-rc2"). Recently, commit d47151b79e32 ("nfs: expose /proc/net/sunrpc/nfs in net namespaces") converted the procfs to per-netns and made the problem more visible. Even when rpc_proc_register() fails, nfs_net_init() could succeed, and thus nfs_net_exit() will be called while destroying the netns. Then, remove_proc_entry() will be called for non-existing proc directory and trigger the warning below. Let's handle the error of rpc_proc_register() properly in nfs_net_init(). [0]: name 'nfs' WARNING: CPU: 1 PID: 1710 at fs/proc/generic.c:711 remove_proc_entry+0x1bb/0x2d0 fs/proc/generic.c:711 Modules linked in: CPU: 1 PID: 1710 Comm: syz-executor.2 Not tainted 6.8.0-12822-gcd51db110a7e #12 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.0-0-gd239552ce722-prebuilt.qemu.org 04/01/2014 RIP: 0010:remove_proc_entry+0x1bb/0x2d0 fs/proc/generic.c:711 Code: 41 5d 41 5e c3 e8 85 09 b5 ff 48 c7 c7 88 58 64 86 e8 09 0e 71 02 e8 74 09 b5 ff 4c 89 e6 48 c7 c7 de 1b 80 84 e8 c5 ad 97 ff <0f> 0b eb b1 e8 5c 09 b5 ff 48 c7 c7 88 58 64 86 e8 e0 0d 71 02 eb RSP: 0018:ffffc9000c6d7ce0 EFLAGS: 00010286 RAX: 0000000000000000 RBX: ffff8880422b8b00 RCX: ffffffff8110503c RDX: ffff888030652f00 RSI: ffffffff81105045 RDI: 0000000000000001 RBP: 0000000000000000 R08: 0000000000000001 R09: 0000000000000000 R10: 0000000000000001 R11: ffffffff81bb62cb R12: ffffffff84807ffc R13: ffff88804ad6fcc0 R14: ffffffff84807ffc R15: ffffffff85741ff8 FS: 00007f30cfba8640(0000) GS:ffff88807dd00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007ff51afe8000 CR3: 000000005a60a005 CR4: 0000000000770ef0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <TASK> rpc_proc_unregister+0x64/0x70 net/sunrpc/stats.c:310 nfs_net_exit+0x1c/0x30 fs/nfs/inode.c:2438 ops_exit_list+0x62/0xb0 net/core/net_namespace.c:170 setup_net+0x46c/0x660 net/core/net_namespace.c:372 copy_net_ns+0x244/0x590 net/core/net_namespace.c:505 create_new_namespaces+0x2ed/0x770 kernel/nsproxy.c:110 unshare_nsproxy_namespaces+0xae/0x160 kernel/nsproxy.c:228 ksys_unshare+0x342/0x760 kernel/fork.c:3322 __do_sys_unshare kernel/fork.c:3393 [inline] __se_sys_unshare kernel/fork.c:3391 [inline] __x64_sys_unshare+0x1f/0x30 kernel/fork.c:3391 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0x4f/0x110 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x46/0x4e RIP: 0033:0x7f30d0febe5d Code: ff c3 66 2e 0f 1f 84 00 00 00 00 00 90 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 73 9f 1b 00 f7 d8 64 89 01 48 RSP: 002b:00007f30cfba7cc8 EFLAGS: 00000246 ORIG_RAX: 0000000000000110 RAX: ffffffffffffffda RBX: 00000000004bbf80 RCX: 00007f30d0febe5d RDX: 0000000000000000 RSI: 0000000000000000 RDI: 000000006c020600 RBP: 00000000004bbf80 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000002 R13: 000000000000000b R14: 00007f30d104c530 R15: 0000000000000000 </TASK>	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36937	In the Linux kernel, the following vulnerability has been resolved: xdp: use flags field to disambiguate broadcast redirect When redirecting a packet using XDP, the bpf_redirect_map() helper will set up the redirect destination information in struct bpf_redirect_info (using the __bpf_xdp_redirect_map() helper function), and the xdp_do_redirect() function will read this information after the XDP program returns and pass the frame on to the right redirect destination. When using the BPF_F_BROADCAST flag to do multicast redirect to a whole map, __bpf_xdp_redirect_map() sets the 'map' pointer in struct bpf_redirect_info to point to the destination map to be broadcast. And xdp_do_redirect() reacts to the value of this map pointer to decide whether it's dealing with a broadcast or a single-value redirect. However, if the destination map is being destroyed before xdp_do_redirect() is called, the map pointer will be cleared out (by bpf_clear_redirect_map()) without waiting for any XDP programs to stop running. This causes xdp_do_redirect() to think that the redirect was to a single target, but the target pointer is also NULL (since broadcast redirects don't have a single target), so this causes a crash when a NULL pointer is passed to dev_map_enqueue(). To fix this, change xdp_do_redirect() to react directly to the presence of the BPF_F_BROADCAST flag in the 'flags' value in struct bpf_redirect_info to disambiguate between a single-target and a broadcast redirect. And only read the 'map' pointer if the broadcast flag is set, aborting if that has been cleared out in the meantime. This prevents the crash, while keeping the atomic (cmpxchg-based) clearing of the map pointer itself, and without adding any more checks in the non-broadcast fast path.	N/A	More Details
CVE-2024-4254	The 'deploy-website.yml' workflow in the gradio-app/gradio repository, specifically in the 'main' branch, is vulnerable to secrets exfiltration due to improper authorization. The vulnerability arises from the workflow's explicit checkout and execution of code from a fork, which is unsafe as it allows the running of untrusted code in an environment with access to push to the base repository and access secrets. This flaw could lead to the exfiltration of sensitive secrets such as GITHUB_TOKEN, HF_TOKEN, VERCEL_ORG_ID, VERCEL_PROJECT_ID, COMMENT_TOKEN, AWSACCESSKEYID, AWSSECRETKEY, and VERCEL_TOKEN. The vulnerability is present in the workflow file located at https://github.com/gradio-app/gradio/blob/72f4ca88ab569aae47941b3fb0609e57f2e13a27/.github/workflows/deploy-website.yml.	N/A	More Details
CVE-2024-36940	In the Linux kernel, the following vulnerability has been resolved: pinctrl: core: delete incorrect free in pinctrl_enable() The "pctldev" struct is allocated in devm_pinctrl_register_and_init(). It's a devm_ managed pointer that is freed by devm_pinctrl_dev_release(), so freeing it in pinctrl_enable() will lead to a double free. The devm_pinctrl_dev_release() function frees the pindescs and destroys the mutex as well.	N/A	More Details
CVE-2024-36960	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: Fix invalid reads in fence signaled events Correctly set the length of the drm_event to the size of the structure that's actually used. The length of the drm_event was set to the parent structure instead of to the drm_vmw_event_fence which is supposed to be read. drm_read uses the length parameter to copy the event to the user space thus resuling in oob reads.	N/A	More Details
CVE-2024-29848	An unrestricted file upload vulnerability in web component of Ivanti Avalanche before 6.4.x allows an authenticated, privileged user to execute arbitrary commands as SYSTEM.	N/A	More Details
CVE-2024-5144	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-4342. Reason: This candidate is a reservation duplicate of CVE-2024-4342. Notes: All CVE users should reference CVE-2024-4342 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-5176	Insufficiently Protected Credentials vulnerability in Baxter Welch Allyn Configuration Tool may allow Remote Services with Stolen Credentials.This issue affects Welch Allyn Configuration Tool: versions 1.9.4.1 and prior.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23316	HTTP request desynchronization in Ping Identity PingAccess, all versions prior to 8.0.1 affected allows an attacker to send specially crafted http header requests to create a request smuggling condition for proxied requests.	N/A	More Details
CVE-2024-33998	Insufficient escaping of participants' names in the participants page table resulted in a stored XSS risk when interacting with some features.	N/A	More Details
CVE-2024-34004	In a shared hosting environment that has been misconfigured to allow access to other users' content, a Moodle user with both access to restore wiki modules and direct access to the web server outside of the Moodle webroot could execute a local file include.	N/A	More Details
CVE-2024-4148	A Regular Expression Denial of Service (ReDoS) vulnerability exists in the lunary-ai/lunary application, version 1.2.10. An attacker can exploit this vulnerability by maliciously manipulating regular expressions, which can significantly impact the response time of the application and potentially render it completely non-functional. Specifically, the vulnerability can be triggered by sending a specially crafted request to the application, leading to a denial of service where the application crashes.	N/A	More Details
CVE-2024-2178	A path traversal vulnerability exists in the parisneo/lollms-webui, specifically within the 'copy_to_custom_personas' endpoint in the 'lollms_personalities_infos.py' file. This vulnerability allows attackers to read arbitrary files by manipulating the 'category' and 'name' parameters during the 'Copy to custom personas folder for editing' process. By inserting '../' sequences in these parameters, attackers can traverse the directory structure and access files outside of the intended directory. Successful exploitation results in unauthorized access to sensitive information.	N/A	More Details
CVE-2024-20066	In modem, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is no needed for exploitation. Patch ID: MOLY01267281; Issue ID: MSV-1477.	N/A	More Details
CVE-2024-5422	An uncontrolled resource consumption of file descriptors in SEH Computertechnik utnserver Pro, SEH Computertechnik utnserver ProMAX, SEH Computertechnik INU-100 allows DoS via HTTP.This issue affects utnserver Pro, utnserver ProMAX, INU-100 version 20.1.22 and below.	N/A	More Details
CVE-2024-5421	Missing input validation and OS command integration of the input in the utnserver Pro, utnserver ProMAX, INU-100 web-interface allows authenticated command injection.This issue affects utnserver Pro, utnserver ProMAX, INU-100 version 20.1.22 and below.	N/A	More Details
CVE-2024-5420	Missing input validation in the SEH Computertechnik utnserver Pro, SEH Computertechnik utnserver ProMAX, SEH Computertechnik INU-100 web-interface allows stored Cross-Site Scripting (XSS)..This issue affects utnserver Pro, utnserver ProMAX, INU-100 version 20.1.22 and below.	N/A	More Details
CVE-2024-4253	A command injection vulnerability exists in the gradio-app/gradio repository, specifically within the 'test-functional.yml' workflow. The vulnerability arises due to improper neutralization of special elements used in a command, allowing for unauthorized modification of the base repository or secrets exfiltration. The issue affects versions up to and including '@gradio/video@0.6.12'. The flaw is present in the workflow's handling of GitHub context information, where it echoes the full name of the head repository, the head branch, and the workflow reference without adequate sanitization. This could potentially lead to the exfiltration of sensitive secrets such as 'GITHUB_TOKEN', 'COMMENT_TOKEN', and 'CHROMATIC_PROJECT_TOKEN'.	N/A	More Details
CVE-2024-20075	In eemgpu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08713302; Issue ID: MSV-1393.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36961	In the Linux kernel, the following vulnerability has been resolved: thermal/debugfs: Fix two locking issues with thermal zone debug With the current thermal zone locking arrangement in the debugfs code, user space can open the "mitigations" file for a thermal zone before the zone's debugfs pointer is set which will result in a NULL pointer dereference in tze_seq_start(). Moreover, thermal_debug_tz_remove() is not called under the thermal zone lock, so it can run in parallel with the other functions accessing the thermal zone's struct thermal_debugfs object. Then, it may clear tz->debugfs after one of those functions has checked it and the struct thermal_debugfs object may be freed prematurely. To address the first problem, pass a pointer to the thermal zone's struct thermal_debugfs object to debugfs_create_file() in thermal_debug_tz_add() and make tze_seq_start(), tze_seq_next(), tze_seq_stop(), and tze_seq_show() retrieve it from s->private instead of a pointer to the thermal zone object. This will ensure that tz_debugfs will be valid across the "mitigations" file accesses until thermal_debugfs_remove_id() called by thermal_debug_tz_remove() removes that file. To address the second problem, use tz->lock in thermal_debug_tz_remove() around the tz->debugfs value check (in case the same thermal zone is removed at the same time in two different threads) and its reset to NULL. Cc :6.8+ <stable@vger.kernel.org> # 6.8+	N/A	More Details
CVE-2024-36941	In the Linux kernel, the following vulnerability has been resolved: wifi: nl80211: don't free NULL coalescing rule If the parsing fails, we can dereference a NULL pointer here.	N/A	More Details
CVE-2024-36963	In the Linux kernel, the following vulnerability has been resolved: tracefs: Reset permissions on remount if permissions are options There's an inconsistency with the way permissions are handled in tracefs. Because the permissions are generated when accessed, they default to the root inode's permission if they were never set by the user. If the user sets the permissions, then a flag is set and the permissions are saved via the inode (for tracefs files) or an internal attribute field (for eventfs). But if a remount happens that specify the permissions, all the files that were not changed by the user gets updated, but the ones that were are not. If the user were to remount the file system with a given permission, then all files and directories within that file system should be updated. This can cause security issues if a file's permission was updated but the admin forgot about it. They could incorrectly think that remounting with permissions set would update all files, but miss some. For example: # cd /sys/kernel/tracing # chgrp 1002 current_tracer # ls -l [..] -rw-r----- 1 root root 0 May 1 21:25 buffer_size_kb -rw-r----- 1 root root 0 May 1 21:25 buffer_subbuf_size_kb -r--r----- 1 root root 0 May 1 21:25 buffer_total_size_kb -rw-r----- 1 root lkp 0 May 1 21:25 current_tracer -rw-r----- 1 root root 0 May 1 21:25 dynamic_events -r--r----- 1 root root 0 May 1 21:25 dyn_ftrace_total_info -r--r----- 1 root root 0 May 1 21:25 enabled_functions Where current_tracer now has group "lkp". # mount -o remount,gid=1001 . # ls -l -rw-r----- 1 root tracing 0 May 1 21:25 buffer_size_kb -rw-r----- 1 root tracing 0 May 1 21:25 buffer_subbuf_size_kb -r--r----- 1 root tracing 0 May 1 21:25 buffer_total_size_kb -rw-r----- 1 root lkp 0 May 1 21:25 current_tracer -rw-r----- 1 root tracing 0 May 1 21:25 dynamic_events -r--r----- 1 root tracing 0 May 1 21:25 dyn_ftrace_total_info -r--r----- 1 root tracing 0 May 1 21:25 enabled_functions Everything changed but the "current_tracer". Add a new link list that keeps track of all the tracefs_inodes which has the permission flags that tell if the file/dir should use the root inode's permission or not. Then on remount, clear all the flags so that the default behavior of using the root inode's permission is done for all files and directories.	N/A	More Details
CVE-2024-36964	In the Linux kernel, the following vulnerability has been resolved: fs/9p: only translate RWX permissions for plain 9P2000 Garbage in plain 9P2000's perm bits is allowed through, which causes it to be able to set (among others) the suid bit. This was presumably not the intent since the unix extended bits are handled explicitly and conditionally on .u.	N/A	More Details
CVE-2024-3829	qdrant/qdrant version 1.9.0-dev is vulnerable to arbitrary file read and write during the snapshot recovery process. Attackers can exploit this vulnerability by manipulating snapshot files to include symlinks, leading to arbitrary file read by adding a symlink that points to a desired file on the filesystem and arbitrary file write by including a symlink and a payload file in the snapshot's directory structure. This vulnerability allows for the reading and writing of arbitrary files on the server, which could potentially lead to a full takeover of the system. The issue is fixed in version v1.9.0.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0336	Improper Access Control vulnerability in EMTA Grup PDKS allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PDKS: before 20240603. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	More Details
CVE-2024-36729	TRENDnet TEW-827DRU devices through 2.06B04 contain a stack-based buffer overflow in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action wizard_ipv6 with a sufficiently long reboot_type key.	N/A	More Details
CVE-2024-5197	There exists interger overflows in libvpx in versions prior to 1.14.1. Calling vpx_img_alloc() with a large value of the d_w, d_h, or align parameter may result in integer overflows in the calculations of buffer sizes and offsets and some fields of the returned vpx_image_t struct may be invalid. Calling vpx_img_wrap() with a large value of the d_w, d_h, or stride_align parameter may result in integer overflows in the calculations of buffer sizes and offsets and some fields of the returned vpx_image_t struct may be invalid. We recommend upgrading to version 1.14.1 or beyond	N/A	More Details
CVE-2024-4332	An authentication bypass vulnerability has been identified in the REST and SOAP API components of Tripwire Enterprise (TE) 9.1.0 when TE is configured to use LDAP/Active Directory SAML authentication and its optional "Auto-synchronize LDAP Users, Roles, and Groups" feature is enabled. This vulnerability allows unauthenticated attackers to bypass authentication if a valid username is known. Exploitation of this vulnerability could allow remote attackers to gain privileged access to the APIs and lead to unauthorized information disclosure or modification.	N/A	More Details
CVE-2022-1242	Apport can be tricked into connecting to arbitrary sockets as the root user	N/A	More Details
CVE-2024-5214	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-5387	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-5388	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-0757	The Insert or Embed Articulate Content into WordPress plugin through 4.3000000023 is not properly filtering which file extensions are allowed to be imported on the server, allowing the uploading of malicious code within zip files	N/A	More Details
CVE-2024-4180	The Events Calendar WordPress plugin before 6.4.0.1 does not properly sanitize user-submitted content when rendering some views via AJAX.	N/A	More Details
CVE-2024-4750	The buddyboss-platform WordPress plugin before 2.6.0 contains an IDOR vulnerability that allows a user to like a private post by manipulating the ID included in the request	N/A	More Details
CVE-2024-22060	An unrestricted file upload vulnerability in web component of Ivanti Neurons for ITSM allows a remote, authenticated, high privileged user to write arbitrary files into sensitive directories of ITSM server.	N/A	More Details
CVE-2024-22059	A SQL injection vulnerability in web component of Ivanti Neurons for ITSM allows a remote authenticated user to read/modify/delete information in the underlying database. This may also lead to DoS.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22058	A buffer overflow allows a low privilege user on the local machine that has the EPM Agent installed to execute arbitrary code with elevated permissions in Ivanti EPM 2021.1 and older.	N/A	More Details
CVE-2024-1275	Use of Default Cryptographic Key vulnerability in Baxter Welch Allyn Connex Spot Monitor may allow Configuration/Environment Manipulation.This issue affects Welch Allyn Connex Spot Monitor in all versions prior to 1.52.	N/A	More Details
CVE-2024-4856	The FS Product Inquiry WordPress plugin through 1.1.1 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin or unauthenticated users	N/A	More Details
CVE-2024-36942	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: qca: fix firmware check error path A recent commit fixed the code that parses the firmware files before downloading them to the controller but introduced a memory leak in case the sanity checks ever fail. Make sure to free the firmware buffer before returning on errors.	N/A	More Details
CVE-2024-36943	In the Linux kernel, the following vulnerability has been resolved: fs/proc/task_mmu: fix loss of young/dirty bits during pagemap scan make_uffd_wp_pte() was previously doing: pte = ptep_get(ptep); ptep_modify_prot_start(ptep); pte = pte_mkuffd_wp(pte); ptep_modify_prot_commit(ptep, pte); But if another thread accessed or dirtied the pte between the first 2 calls, this could lead to loss of that information. Since ptep_modify_prot_start() gets and clears atomically, the following is the correct pattern and prevents any possible race. Any access after the first call would see an invalid pte and cause a fault: pte = ptep_modify_prot_start(ptep); pte = pte_mkuffd_wp(pte); ptep_modify_prot_commit(ptep, pte);	N/A	More Details
CVE-2024-36945	In the Linux kernel, the following vulnerability has been resolved: net/smc: fix neighbour and rtable leak in smc_ib_find_route() In smc_ib_find_route(), the neighbour found by neigh_lookup() and rtable resolved by ip_route_output_flow() are not released or put before return. It may cause the refcount leak, so fix it.	N/A	More Details
CVE-2024-36946	In the Linux kernel, the following vulnerability has been resolved: phonet: fix rtm_phonet_notify() skb allocation fill_route() stores three components in the skb: - struct rtmsg - RTA_DST (u8) - RTA_OIF (u32) Therefore, rtm_phonet_notify() should use NLMSG_ALIGN(sizeof(struct rtmsg)) + nla_total_size(1) + nla_total_size(4)	N/A	More Details
CVE-2024-36948	In the Linux kernel, the following vulnerability has been resolved: drm/xe/xe_migrate: Cast to output precision before multiplying operands Addressing potential overflow in result of multiplication of two lower precision (u32) operands before widening it to higher precision (u64). -v2 Fix commit message and description. (Rodrigo) (cherry picked from commit 34820967ae7b45411f8f4f737c2d63b0c608e0d7)	N/A	More Details
CVE-2024-36949	In the Linux kernel, the following vulnerability has been resolved: amd/amdkfd: sync all devices to wait all processes being evicted If there are more than one device doing reset in parallel, the first device will call kfd_suspend_all_processes() to evict all processes on all devices, this call takes time to finish. other device will start reset and recover without waiting. if the process has not been evicted before doing recover, it will be restored, then caused page fault.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36950	In the Linux kernel, the following vulnerability has been resolved: firewire: ohci: mask bus reset interrupts between ISR and bottom half In the FireWire OHCI interrupt handler, if a bus reset interrupt has occurred, mask bus reset interrupts until bus_reset_work has serviced and cleared the interrupt. Normally, we always leave bus reset interrupts masked. We infer the bus reset from the self-ID interrupt that happens shortly thereafter. A scenario where we unmask bus reset interrupts was introduced in 2008 in a007bb857e0b26f5d8b73c2ff90782d9c0972620: If OHCI_PARAM_DEBUG_BUSRESETS (8) is set in the debug parameter bitmask, we will unmask bus reset interrupts so we can log them. irq_handler logs the bus reset interrupt. However, we can't clear the bus reset event flag in irq_handler, because we won't service the event until later. irq_handler exits with the event flag still set. If the corresponding interrupt is still unmasked, the first bus reset will usually freeze the system due to irq_handler being called again each time it exits. This freeze can be reproduced by loading firewire_ohci with "modprobe firewire_ohci debug=-1" (to enable all debugging output). Apparently there are also some cases where bus_reset_work will get called soon enough to clear the event, and operation will continue normally. This freeze was first reported a few months after a007bb85 was committed, but until now it was never fixed. The debug level could safely be set to -1 through sysfs after the module was loaded, but this would be ineffectual in logging bus reset interrupts since they were only unmasked during initialization. irq_handler will now leave the event flag set but mask bus reset interrupts, so irq_handler won't be called again and there will be no freeze. If OHCI_PARAM_DEBUG_BUSRESETS is enabled, bus_reset_work will unmask the interrupt after servicing the event, so future interrupts will be caught as desired. As a side effect to this change, OHCI_PARAM_DEBUG_BUSRESETS can now be enabled through sysfs in addition to during initial module loading. However, when enabled through sysfs, logging of bus reset interrupts will be effective only starting with the second bus reset, after bus_reset_work has executed.	N/A	More Details
CVE-2024-36951	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: range check cp bad op exception interrupts Due to a CP interrupt bug, bad packet garbage exception codes are raised. Do a range check so that the debugger and runtime do not receive garbage codes. Update the user api to guard exception code type checking as well.	N/A	More Details
CVE-2024-36952	In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Move NPIV's transport unregistration to after resource clean up There are cases after NPIV deletion where the fabric switch still believes the NPIV is logged into the fabric. This occurs when a vport is unregistered before the Remove All DA_ID CT and LOGO ELS are sent to the fabric. Currently fc_remove_host(), which calls dev_loss_tmo for all D_IDs including the fabric D_ID, removes the last ndlp reference and frees the ndlp rport object. This sometimes causes the race condition where the final DA_ID and LOGO are skipped from being sent to the fabric switch. Fix by moving the fc_remove_host() and scsi_remove_host() calls after DA_ID and LOGO are sent.	N/A	More Details
CVE-2024-36954	In the Linux kernel, the following vulnerability has been resolved: tipc: fix a possible memleak in tipc_buf_append __skb_linearize() doesn't free the skb when it fails, so move '*buf = NULL' after __skb_linearize(), so that the skb can be freed on the err path.	N/A	More Details
CVE-2024-36956	In the Linux kernel, the following vulnerability has been resolved: thermal/debugfs: Free all thermal zone debug memory on zone removal Because thermal_debug_tz_remove() does not free all memory allocated for thermal zone diagnostics, some of that memory becomes unreachable after freeing the thermal zone's struct thermal_debugfs object. Address this by making thermal_debug_tz_remove() free all of the memory in question. Cc :6.8+ <stable@vger.kernel.org> # 6.8+	N/A	More Details
CVE-2024-36957	In the Linux kernel, the following vulnerability has been resolved: octeontx2-af: avoid off-by-one read from userspace We try to access count + 1 byte from userspace with memdup_user(buffer, count + 1). However, the userspace only provides buffer of count bytes and only these count bytes are verified to be okay to access. To ensure the copied buffer is NUL terminated, we use memdup_user_nul instead.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36958	In the Linux kernel, the following vulnerability has been resolved: NFSD: Fix nfsd4_encode_fattr4() crasher Ensure that args.acl is initialized early. It is used in an unconditional call to kfree() on the way out of nfsd4_encode_fattr4().	N/A	More Details
CVE-2024-36959	In the Linux kernel, the following vulnerability has been resolved: pinctrl: devicetree: fix refcount leak in pinctrl_dt_to_map() If we fail to allocate propname buffer, we need to drop the reference count we just took. Because the pinctrl_dt_free_maps() includes the droping operation, here we call it directly.	N/A	More Details
CVE-2024-5537	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-2420	LenelS2 NetBox access control and event monitoring system was discovered to contain Hardcoded Credentials in versions prior to and including 5.6.1 which allows an attacker to bypass authentication requirements.	N/A	More Details
CVE-2024-2421	LenelS2 NetBox access control and event monitoring system was discovered to contain an unauthenticated RCE in versions prior to and including 5.6.1, which allows an attacker to execute malicious commands with elevated permissions.	N/A	More Details
CVE-2024-2422	LenelS2 NetBox access control and event monitoring system was discovered to contain an authenticated RCE in versions prior to and including 5.6.1, which allows an attacker to execute malicious commands.	N/A	More Details
CVE-2024-4842	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: Not a vulnerability	N/A	More Details
CVE-2024-37032	Ollama before 0.1.34 does not validate the format of the digest (sha256 with 64 hex digits) when getting the model path, and thus mishandles the TestGetBlobsPath test cases such as fewer than 64 hex digits, more than 64 hex digits, or an initial ../ substring.	N/A	More Details
CVE-2024-4469	The WP STAGING WordPress Backup Plugin WordPress plugin before 3.5.0 does not prevent users with the administrator role from pinging conducting SSRF attacks, which may be a problem in multisite configurations.	N/A	More Details
CVE-2024-5436	Type confusion in Snapchat LensCore could lead to denial of service or arbitrary code execution prior to version 12.88. We recommend upgrading to version 12.88 or above.	N/A	More Details
CVE-2024-5484	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-5538	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-1980	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-6876. Reason: This candidate is a reservation duplicate of CVE-2023-6876. Notes: All CVE users should reference CVE-2023-6876 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-38042	A local privilege escalation vulnerability in Ivanti Secure Access Client for Windows allows a low privileged user to execute code as SYSTEM.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38551	A CRLF Injection vulnerability in Ivanti Connect Secure (9.x, 22.x) allows an authenticated high-privileged user to inject malicious code on a victim's browser, thereby leading to cross-site scripting attack.	N/A	More Details
CVE-2023-46810	A local privilege escalation vulnerability in Ivanti Secure Access Client for Linux before 22.7R1, allows a low privileged user to execute code as root.	N/A	More Details
CVE-2020-27353	Rejected reason: CVE ID was once reserved, but never used.	N/A	More Details