https://nciipc.gov.in

National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

16 - 31 Jan 2025 Vol. 12 No. 02

Table of Content

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 07fly					
Product: 07flycms					
Affected Version(s): 1.3.9					
Cross-Site Request Forgery (CSRF)	16-Jan-2025	4.3	07FLYCMS V1.3.9 was discovered to contain a Cross-Site Request Forgery (CSRF) via /erp.07fly.net:80/oa/OaTask/edit.html. **CVE ID: CVE-2024-57160**	N/A	A-07F-07FL-040225/1
Cross-Site Request Forgery (CSRF)	16-Jan-2025	4.3	07FLYCMS V1.3.9 was discovered to contain a Cross-Site Request Forgery (CSRF) via /erp.07fly.net:80/oa/OaWorkReport/edit.html **CVE ID: CVE-2024-57161**	N/A	A-07F-07FL-040225/2
Vendor: aakashbhagat					
Product: single_user_chat					
Affected Version(s): * Up to (including) 0.5					
Improper Authorization	30-Jan-2025	8.1	The Single-user-chat plugin for WordPress is vulnerable to unauthorized modification of data that can lead to a denial of service due to insufficient validation on the 'single_user_chat_update_login' function in all versions up to, and including, 0.5. This makes it possible for authenticated attackers, with subscriber-level access and above, to update option values to 'login' on the WordPress site. This may be leveraged to update an option that would create an error on the site and deny service to legitimate users or be used to set some	N/A	A-AAK-SING-040225/3

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			values to true such as registration. **CVE ID: CVE-2024-13646**		
Vendor: aipower					
Product: aipower					
Affected Version(s): * Up to (excluding) 1.8.97					
Deserialization of Untrusted Data	22-Jan-2025	7.2	The "AI Power: Complete AI Pack" plugin for WordPress is vulnerable to PHP Object Injection in versions up to, and including, 1.8.96 via deserialization of untrusted input from the $form['post_content'] variable through the wpaicg_export_ai_forms() function. This allows authenticated attackers, with administrative privileges, to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code. **CVE ID: CVE-2025-0429**	https://plugins.trac.wordpress.org/changeset/3224162/	A-AIP-AIPO-040225/4
Deserialization of Untrusted Data	22-Jan-2025	7.2	The "AI Power: Complete AI Pack" plugin for WordPress is vulnerable to PHP Object Injection in versions up to, and including, 1.8.96 via deserialization of untrusted input from the $form['post_content'] variable through the wpaicg_export_prompts function. This allows authenticated attackers, with administrative privileges, to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is	https://plugins.trac.wordpress.org/changeset/3224162/	A-AIP-AIPO-040225/5

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code. **CVE ID: CVE-2025-0428**		
Missing Authorization	22-Jan-2025	6.3	The AI Power: Complete AI Pack plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the wpaicg_save_image_media function in all versions up to, and including, 1.8.96. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload image files and embed shortcode attributes in the image_alt value that will execute when sending a POST request to the attachment page. **CVE ID: CVE-2024-13361**	https://plugins.trac.wordpress.org/changeset/3224162/gpt3-ai-content-generator/trunk/classes/wpaicg_image.php	A-AIP-AIPO-040225/6
Server-Side Request Forgery (SSRF)	22-Jan-2025	5.4	The AI Power: Complete AI Pack plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.8.96 via the wpaicg_troubleshoot_add_vector(). This makes it possible for authenticated attackers, with subscriber-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services. **CVE ID: CVE-2024-13360**	https://plugins.trac.wordpress.org/changeset/3224162/	A-AIP-AIPO-040225/7

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Apple					
Product: safari					
Affected Version(s): * Up to (excluding) 18.2					
Out-of-bounds Write	27-Jan-2025	8.8	The issue was addressed with improved memory handling. This issue is fixed in visionOS 2.2, tvOS 18.2, Safari 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sequoia 15.2. Processing maliciously crafted web content may lead to memory corruption. **CVE ID: CVE-2024-54543**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845, https://support.apple.com/en-us/121846	A-APP-SAFA-040225/8
Affected Version(s): * Up to (excluding) 18.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Jan-2025	8.8	A privacy issue was addressed with improved handling of files. This issue is fixed in macOS Sequoia 15.3, Safari 18.3, iOS 18.3 and iPadOS 18.3. Copying a URL from Web Inspector may lead to command injection. **CVE ID: CVE-2025-24150**	N/A	A-APP-SAFA-040225/9
N/A	27-Jan-2025	7.5	A logging issue was addressed with improved data redaction. This issue is fixed in macOS Sequoia 15.3, Safari 18.3. A malicious app may be able to bypass browser extension authentication. **CVE ID: CVE-2025-24169**	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122074	A-APP-SAFA-040225/10
N/A	27-Jan-2025	6.5	The issue was addressed with improved access restrictions to the file system. This issue is fixed in macOS Sequoia 15.3, Safari 18.3, iOS 18.3 and iPadOS	N/A	A-APP-SAFA-040225/11

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			18.3, visionOS 2.3. A maliciously crafted webpage may be able to fingerprint the user. **CVE ID: CVE-2025-24143**		
N/A	27-Jan-2025	4.3	The issue was addressed with improved UI. This issue is fixed in macOS Sequoia 15.3, Safari 18.3, iOS 18.3 and iPadOS 18.3, visionOS 2.3. Visiting a malicious website may lead to user interface spoofing. **CVE ID: CVE-2025-24113**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122073, https://support.apple.com/en-us/122074	A-APP-SAFA-040225/12
N/A	27-Jan-2025	4.3	The issue was addressed by adding additional logic. This issue is fixed in macOS Sequoia 15.3, Safari 18.3, iOS 18.3 and iPadOS 18.3. Visiting a malicious website may lead to address bar spoofing. **CVE ID: CVE-2025-24128**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122074	A-APP-SAFA-040225/13
Vendor: areoi					
Product: all_bootstrap_blocks					
Affected Version(s): * Up to (excluding) 1.3.27					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Jan-2025	6.4	The All Bootstrap Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the "Accordion" widget in all versions up to, and including, 1.3.26 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	https://plugins.trac.wordpress.org/changeset/3228370/all-bootstrap-blocks/trunk/blocks/accordion-item.php	A-ARE-ALL_-040225/14

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			whenever a user accesses an injected page. **CVE ID: CVE-2024-13549**		
Vendor: atarim					
Product: visual_website_collaboration\,_feedback_\&_project_management					
Affected Version(s): * Up to (excluding) 4.1.0					
Missing Authorization	21-Jan-2025	5.3	The Visual Website Collaboration, Feedback & Project Management – Atarim plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the wpf_delete_file and wpf_delete_file functions in all versions up to, and including, 4.0.9. This makes it possible for unauthenticated attackers to delete project pages and files. **CVE ID: CVE-2024-12104**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3225314%40atarim-visual-collaboration&new=3225314%40atarim-visual-collaboration&sfp_email=&sfph_mail=	A-ATA-VISU-040225/15
Vendor: ayecode					
Product: ketchup_shortcodes					
Affected Version(s): * Up to (excluding) 0.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jan-2025	6.4	The Ketchup Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'spacer' shortcode in all versions up to, and including, 0.1.2 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. **CVE ID: CVE-2024-13590**	https://plugins.trac.wordpress.org/changeset/3222176/	A-AYE-KETC-040225/16

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: bowo					
Product: system_dashboard					
Affected Version(s): * Up to (including) 2.8.15					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Jan-2025	6.1	The System Dashboard plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the Filename parameter in all versions up to, and including, 2.8.15 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick an administrative user into performing an action such as clicking on a link. **CVE ID: CVE-2024-12299**	N/A	A-BOW-SYST-040225/17
Vendor: cliptakes					
Product: cliptakes					
Affected Version(s): * Up to (excluding) 1.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2025	6.4	The Cliptakes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'cliptakes_input_email' shortcode 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. **CVE ID: CVE-2024-13389**	https://plugins.trac.wordpress.org/changeset/3226472/cliptakes/tags/1.3.5/public/class-cliptakes-public.php	A-CLI-CLIP-040225/18

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: crocoblock					
Product: jetelements					
Affected Version(s): * Up to (excluding) 2.7.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jan-2025	6.4	The JetElements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several widgets in all versions up to, and including, 2.7.2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2025-0371**	N/A	A-CRO-JETE-040225/19
Vendor: cyberchimps					
Product: responsive_blocks					
Affected Version(s): * Up to (excluding) 2.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Jan-2025	6.4	The Responsive Blocks – WordPress Gutenberg Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'section_tag' parameter in all versions up to, and including, 1.9.9 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. **CVE ID: CVE-2024-13732**	https://plugins.trac.wordpress.org/changeset/3231017/	A-CYB-RESP-040225/20

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: dwbooster					
Product: cp_contact_form					
Affected Version(s): * Up to (excluding) 1.3.53					
Cross-Site Request Forgery (CSRF)	30-Jan-2025	6.5	The CP Contact Form with PayPal plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.3.52. This is due to missing or incorrect nonce validation on the cp_contact_form_paypal_check_init_actions() function. This makes it possible for unauthenticated attackers to add discount codes via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2024-13758**	https://plugins.trac.wordpress.org/changeset/3230873/	A-DWB-CP_C-040225/21
Vendor: ecpay					
Product: ecpay_ecommerce_for_woocommerce					
Affected Version(s): * Up to (including) 1.1.2411060					
Missing Authorization	30-Jan-2025	4.3	The ECPay Ecommerce for WooCommerce plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'clear_ecpay_debug_log' AJAX action in all versions up to, and including, 1.1.2411060. This makes it possible for authenticated attackers, with Subscriber-level access and above, to clear the plugin's log files. **CVE ID: CVE-2024-13652**	N/A	A-ECP-ECPA-040225/22
Vendor: Elastic					
Product: elasticsearch					
Affected Version(s): From (including) 7.17.0 Up to (excluding) 7.17.21					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	21-Jan-2025	6.5	An allocation of resources without limits or throttling in Elasticsearch can lead to an OutOfMemoryError exception resulting in a crash via a specially crafted query using an SQL function. **CVE ID: CVE-2024-43709**	https://discuss.elastic.co/t/elasticsearch-7-17-21-and-8-13-3-security-update-esa-2024-25/373442	A-ELA-ELAS-040225/23
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.13.3					
Allocation of Resources Without Limits or Throttling	21-Jan-2025	6.5	An allocation of resources without limits or throttling in Elasticsearch can lead to an OutOfMemoryError exception resulting in a crash via a specially crafted query using an SQL function. **CVE ID: CVE-2024-43709**	https://discuss.elastic.co/t/elasticsearch-7-17-21-and-8-13-3-security-update-esa-2024-25/373442	A-ELA-ELAS-040225/24
Vendor: elementor					
Product: website_builder					
Affected Version(s): * Up to (excluding) 3.25.11					
Exposure of Sensitive Information to an Unauthorized Actor	30-Jan-2025	4.3	The Elementor Website Builder Pro plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.25.10 via the 'elementor-template' shortcode. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive data including the content of Private, Pending, and Draft Templates. The vulnerability was partially patched in version 3.24.4. **CVE ID: CVE-2024-8494**	N/A	A-ELE-WEBS-040225/25
Vendor: gambit					
Product: stackable					
Affected Version(s): * Up to (excluding) 3.13.12					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jan-2025	6.4	The Stackable – Page Builder Gutenberg Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title' parameter of the Button block in all versions up to, and including, 3.13.11 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. **CVE ID: CVE-2024-12117**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3223387%40stackable-ultimate-gutenberg-blocks&new=3223387%40stackable-ultimate-gutenberg-blocks&sfp_email=&sfph_mail=	A-GAM-STAC-040225/26
Vendor: gamipress					
Product: gamipress					
Affected Version(s): * Up to (excluding) 7.2.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Jan-2025	7.5	The GamiPress – Gamification plugin to reward points, achievements, badges & ranks in WordPress plugin for WordPress is vulnerable to time-based SQL Injection via the 'orderby' parameter in all versions up to, and including, 7.2.1 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. **CVE ID: CVE-2024-13496**	https://plugins.trac.wordpress.org/browser/gamipress/trunk/includes/ajax-functions.php#L39, https://plugins.trac.wordpress.org/browser/gamipress/trunk/libraries/ct/includes/class-ct-query.php#L160, https://plugins.trac.wordpress.org/changeset/3226227/	A-GAM-GAMI-040225/27

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	22-Jan-2025	7.3	The The GamiPress – Gamification plugin to reward points, achievements, badges & ranks in WordPress plugin for WordPress is vulnerable to arbitrary shortcode execution via gamipress_do_shortcode() function in all versions up to, and including, 7.2.1. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes. **CVE ID: CVE-2024-13499**	https://plugins.trac.wordpress.org/browser/gamipress/trunk/includes/functions.php, https://plugins.trac.wordpress.org/browser/gamipress/trunk/includes/functions.php#L645, https://plugins.trac.wordpress.org/changeset/3226227/	A-GAM-GAMI-040225/28
Improper Control of Generation of Code ('Code Injection')	22-Jan-2025	7.3	The The GamiPress – Gamification plugin to reward points, achievements, badges & ranks in WordPress plugin for WordPress is vulnerable to arbitrary shortcode execution via the gamipress_ajax_get_logs() function in all versions up to, and including, 7.2.1. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes. **CVE ID: CVE-2024-13495**	https://plugins.trac.wordpress.org/changeset/3226227/	A-GAM-GAMI-040225/29
Vendor: gubbigubbi					
Product: kona_gallery_block					
Affected Version(s): * Up to (including) 1.7					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Jan-2025	6.4	The Kona Gallery Block plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the "Kona: Instagram for Gutenberg" Block, specifically in the "align" attribute, in all versions up to, and including, 1.7 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. **CVE ID: CVE-2024-13400**	N/A	A-GUB-KONA-040225/30
Vendor: hirewebxperts					
Product: passwords_manager					
Affected Version(s): * Up to (excluding) 1.5.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jan-2025	7.5	The Passwords Manager plugin for WordPress is vulnerable to SQL Injection via the $wpdb->prefix value in several AJAX fuctions in all versions up to, and including, 1.4.8 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. **CVE ID: CVE-2024-12613**	https://plugins.trac.wordpress.org/changeset/3221505/passwords-manager/trunk/include/pms-passwords-ajax-action.php	A-HIR-PASS-040225/31
Improper Neutralization of Special	16-Jan-2025	7.5	The Passwords Manager plugin for WordPress is vulnerable to unauthorized	https://plugins.trac.wordpress.org/changeset/3	A-HIR-PASS-040225/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			modification of data due to a missing capability check on the 'pms_save_setting' and 'post_new_pass' AJAX actions in all versions up to, and including, 1.4.8. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update the plugins settings and add passwords. **CVE ID: CVE-2024-12614**	221505/passwords-manager/trunk/include/pms-passwords-ajax-action.php, https://plugins.trac.wordpress.org/changeset/3221505/passwords-manager/trunk/include/pms-settings-ajax-action.php	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jan-2025	6.5	The Passwords Manager plugin for WordPress is vulnerable to SQL Injection via the $wpdb->prefix value in several AJAX actions in all versions up to, and including, 1.4.8 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID: CVE-2024-12615**	https://plugins.trac.wordpress.org/changeset/3221505/passwords-manager/trunk/include/admin-page/addon/csv-export/index.php, https://plugins.trac.wordpress.org/changeset/3221505/passwords-manager/trunk/include/pms-categories-ajax-action.php	A-HIR-PASS-040225/33
Vendor: IBM					
Product: security_verify_access					
Affected Version(s): From (including) 10.0.0 Up to (including) 10.0.8					
Unverified Password Change	20-Jan-2025	5.6	IBM Security Verify Access 10.0.0 through 10.0.8 and IBM Security Verify Access Docker 10.0.0 through 10.0.8 could allow could an unverified user to change the password of an expired user without prior	https://www.ibm.com/support/pages/node/7176212	A-IBM-SECU-040225/34

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			knowledge of that password. **CVE ID: CVE-2024-45647**		
Product: security_verify_access_docker					
Affected Version(s): From (including) 10.0.0 Up to (including) 10.0.8					
Unverified Password Change	20-Jan-2025	5.6	IBM Security Verify Access 10.0.0 through 10.0.8 and IBM Security Verify Access Docker 10.0.0 through 10.0.8 could allow could an unverified user to change the password of an expired user without prior knowledge of that password. **CVE ID: CVE-2024-45647**	https://www.ibm.com/support/pages/node/7176212	A-IBM-SECU-040225/35
Product: urbancode_deploy					
Affected Version(s): From (including) 7.0.0.0 Up to (excluding) 7.0.5.25					
Insertion of Sensitive Information into Log File	21-Jan-2025	6.2	IBM UrbanCode Deploy (UCD) 7.0 through 7.0.5.24, 7.1 through 7.1.2.10, and 7.2 through 7.2.3.13 stores potentially sensitive information in log files that could be read by a local user with access to HTTP request logs. **CVE ID: CVE-2024-45091**	https://www.ibm.com/support/pages/node/7177857	A-IBM-URBA-040225/36
Affected Version(s): From (including) 7.1.0.0 Up to (excluding) 7.1.2.21					
Insertion of Sensitive Information into Log File	21-Jan-2025	6.2	IBM UrbanCode Deploy (UCD) 7.0 through 7.0.5.24, 7.1 through 7.1.2.10, and 7.2 through 7.2.3.13 stores potentially sensitive information in log files that could be read by a local user with access to HTTP request logs. **CVE ID: CVE-2024-45091**	https://www.ibm.com/support/pages/node/7177857	A-IBM-URBA-040225/37
Affected Version(s): From (including) 7.2.0.0 Up to (excluding) 7.2.3.14					
Insertion of Sensitive	21-Jan-2025	6.2	IBM UrbanCode Deploy (UCD) 7.0 through 7.0.5.24, 7.1 through 7.1.2.10, and	https://www.ibm.com/support/	A-IBM-URBA-040225/38

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information into Log File			7.2 through 7.2.3.13 stores potentially sensitive information in log files that could be read by a local user with access to HTTP request logs. **CVE ID: CVE-2024-45091**	pages/node/7177857	
Vendor: icontrolwp					
Product: icontrolwp					
Affected Version(s): * Up to (including) 4.4.5					
Deserialization of Untrusted Data	30-Jan-2025	9.8	The iControlWP – Multiple WordPress Site Manager plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 4.4.5 via deserialization of untrusted input from the reqpars parameter. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present. **CVE ID: CVE-2024-13742**	https://plugins.trac.wordpress.org/browser/worpit-admin-dashboard-plugin/tags/4.4.5/lib/src/LegacyApi/RequestParameters.php#L42, https://plugins.trac.wordpress.org/browser/worpit-admin-dashboard-plugin/tags/4.4.5/src/api/RequestParameters.php#L14	A-ICO-ICON-040225/39
Vendor: icopydoc					
Product: xml_for_google_merchant_center					
Affected Version(s): * Up to (excluding) 3.0.12					
Improper Neutralization of Input During Web Page	22-Jan-2025	6.1	The XML for Google Merchant Center plugin for WordPress is vulnerable to Reflected Cross-Site	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_	A-ICO-XML_-040225/40

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Scripting via the 'feed_id' parameter in all versions up to, and including, 3.0.11 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-13406**	mail=&reponame=&old=322640 3%40xml-for-google-merchant-center&new=32 26403%40xml-for-google-merchant-center&sfp_email=&sfph_mail=	
Vendor: ikjweb					
Product: zstore_manager_basic					
Affected Version(s): * Up to (including) 3.311					
Missing Authorization	30-Jan-2025	4.3	The zStore Manager Basic plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the zstore_clear_cache() function in all versions up to, and including, 3.311. This makes it possible for authenticated attackers, with Subscriber-level access and above, to clear the plugin's cache. **CVE ID: CVE-2024-13715**	https://plugins.trac.wordpress.org/browser/zstore-manager-basic/trunk/zstore-manager.php#L441	A-IKJ-ZSTO-040225/41
Vendor: ilghera					
Product: mailup_auto_subscription					
Affected Version(s): * Up to (excluding) 1.2.0					
Cross-Site Request Forgery (CSRF)	28-Jan-2025	6.1	The MailUp Auto Subscription plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.0. This is due to missing or incorrect nonce validation on the mas_options function. This makes it possible for unauthenticated attackers	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=306007 8%40mailup-auto-subscribtion%2 Ftags%2F1.1.0& new=3229728%	A-ILG-MAIL-040225/42

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2024-13521**	40mailup-auto-subscribtion%2Ftags%2F1.2.0	
Vendor: infinitescript					
Product: wp-bibtex					
Affected Version(s): * Up to (excluding) 3.0.2					
Cross-Site Request Forgery (CSRF)	21-Jan-2025	6.1	The WP-BibTeX plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.0.1. This is due to missing or incorrect nonce validation on the wp_bibtex_option_page() function. This makes it possible for unauthenticated attackers to inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2024-12005**	https://plugins.trac.wordpress.org/changeset/3225023	A-INF-WP-B-040225/43
Vendor: ivanm					
Product: wp_image_uploader					
Affected Version(s): * Up to (including) 1.0.1					
Cross-Site Request Forgery (CSRF)	30-Jan-2025	8.8	The WP Image Uploader plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.1. This is due to missing or incorrect nonce validation on the gky_image_uploader_main_function() function. This makes it possible for unauthenticated attackers to delete arbitrary files via a forged request granted they	https://plugins.trac.wordpress.org/browser/wp-image-uploader/trunk/index.php#L85	A-IVA-WP_I-040225/44

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2024-13707**		
Cross-Site Request Forgery (CSRF)	30-Jan-2025	8.8	The WP Image Uploader plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the gky_image_uploader_main_function() function in all versions up to, and including, 1.0.1. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). **CVE ID: CVE-2024-13720**	https://plugins.trac.wordpress.org/browser/wp-image-uploader/trunk/index.php#L85	A-IVA-WP_I-040225/45
Vendor: Jetbrains					
Product: hub					
Affected Version(s): * Up to (excluding) 2024.3.55417					
Authentication Bypass Using an Alternate Path or Channel	21-Jan-2025	6.7	In JetBrains Hub before 2024.3.55417 privilege escalation was possible via LDAP authentication mapping **CVE ID: CVE-2025-24456**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-HUB-040225/46
Product: teamcity					
Affected Version(s): * Up to (excluding) 2024.12.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jan-2025	4.6	In JetBrains TeamCity before 2024.12.1 reflected XSS was possible on the Vault Connection page **CVE ID: CVE-2025-24459**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-040225/47
Incorrect Authorization	21-Jan-2025	4.3	In JetBrains TeamCity before 2024.12.1 improper access control allowed to	https://www.jetbrains.com/privacy-	A-JET-TEAM-040225/48

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			see Projects' names in the agent pool **CVE ID: CVE-2025-24460**	security/issues-fixed/	
Affected Version(s): 2024.12.1					
Missing Authorization	21-Jan-2025	6.5	In JetBrains TeamCity before 2024.12.1 decryption of connection secrets without proper permissions was possible via Test Connection endpoint **CVE ID: CVE-2025-24461**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-040225/49
Product: youtrack					
Affected Version(s): * Up to (excluding) 2024.3.55417					
Authentication Bypass by Spoofing	21-Jan-2025	7.1	In JetBrains YouTrack before 2024.3.55417 account takeover was possible via spoofed email and Helpdesk integration **CVE ID: CVE-2025-24458**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-YOUT-040225/50
Insertion of Sensitive Information into Log File	21-Jan-2025	5.5	In JetBrains YouTrack before 2024.3.55417 permanent tokens could be exposed in logs **CVE ID: CVE-2025-24457**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-YOUT-040225/51
Vendor: jfinaloa_project					
Product: jfinaloa					
Affected Version(s): * Up to (excluding) 2025-01-01					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jan-2025	8.8	JFinalOA before v2025.01.01 was discovered to contain a SQL injection vulnerability via the component borrowmoney/listData?applyUser. **CVE ID: CVE-2024-57769**	N/A	A-JFI-JFIN-040225/52
Improper Neutralization of Special Elements used in an SQL Command	16-Jan-2025	8.8	JFinalOA before v2025.01.01 was discovered to contain a SQL injection vulnerability via the component getWorkFlowHis?insid.	N/A	A-JFI-JFIN-040225/53

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			**CVE ID: CVE-2024-57775**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jan-2025	8.8	JFinalOA before v2025.01.01 was discovered to contain a SQL injection vulnerability via the component apply/save#oaContractApply.id. **CVE ID: CVE-2024-57770**	N/A	A-JFI-JFIN-040225/54
Vendor: jyothisjoy					
Product: eventer					
Affected Version(s): * Up to (excluding) 3.9.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Jan-2025	7.5	The Eventer plugin for WordPress is vulnerable to SQL Injection via the 'event' parameter in the 'eventer_get_attendees' function in all versions up to, and including, 3.9.8 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. **CVE ID: CVE-2024-11135**	N/A	A-JYO-EVEN-040225/55
Vendor: Linuxfoundation					
Product: magma					
Affected Version(s): * Up to (including) 1.8.0					
Reachable Assertion	21-Jan-2025	7.5	Magma versions <= 1.8.0 (fixed in v1.9 commit 08472ba98b8321f802e95f5622fa90fec2dea486) are susceptible to an assertion-based crash when an oversized NAS packet is received. An attacker may leverage this behavior to	N/A	A-LIN-MAGM-040225/56

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			repeatedly crash the MME via either a compromised base station or via an unauthenticated cellphone within range of a base station managed by the MME, causing a denial of service. **CVE ID: CVE-2023-37029**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-Jan-2025	7.5	The Linux Foundation Magma <= 1.8.0 (fixed in v1.9 commit 08472ba98b8321f802e95f5622fa90fec2dea486) was discovered to contain a buffer overflow in the decode_access_point_name_ie function at /3gpp/3gpp_24.008_sm_ies.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted NAS packet. **CVE ID: CVE-2024-24416**	N/A	A-LIN-MAGM-040225/57
Out-of-bounds Write	21-Jan-2025	7.5	A Stack-based buffer overflow in the Mobile Management Entity (MME) of Magma versions <= 1.8.0 (fixed in v1.9 commit 08472ba98b8321f802e95f5622fa90fec2dea486) allows remote attackers to crash the MME with an unauthenticated cellphone by sending a NAS packet containing an oversized `Emergency Number List` Information Element. **CVE ID: CVE-2023-37032**	N/A	A-LIN-MAGM-040225/58
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-Jan-2025	7.5	The Linux Foundation Magma <= 1.8.0 (fixed in v1.9 commit 08472ba98b8321f802e95f5622fa90fec2dea486) was discovered to contain a buffer overflow in the decode_pdn_address function at	N/A	A-LIN-MAGM-040225/59

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/nas/ies/PdnAddress.cpp. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted NAS packet. **CVE ID: CVE-2024-24418**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-Jan-2025	7.5	The Linux Foundation Magma <= 1.8.0 (fixed in v1.9 commit 08472ba98b8321f802e95f5622fa90fec2dea486) was discovered to contain a buffer overflow in the decode_traffic_flow_template_packet_filter function at /3gpp/3gpp_24.008_sm_ies.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted NAS packet. **CVE ID: CVE-2024-24419**	N/A	A-LIN-MAGM-040225/60
Out-of-bounds Write	21-Jan-2025	7.5	The Linux Foundation Magma <= 1.8.0 (fixed in v1.9 commit 08472ba98b8321f802e95f5622fa90fec2dea486) was discovered to contain a stack overflow in the decode_protocol_configuration_options function at /3gpp/3gpp_24.008_sm_ies.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted NAS packet. **CVE ID: CVE-2024-24422**	N/A	A-LIN-MAGM-040225/61
Out-of-bounds Write	21-Jan-2025	7.5	The Linux Foundation Magma <= 1.8.0 (fixed in v1.9 commit 08472ba98b8321f802e95f5622fa90fec2dea486) was discovered to contain a buffer overflow in the decode_esm_message_container function at /nas/ies/EsmMessageContainer.cpp. This vulnerability allows	N/A	A-LIN-MAGM-040225/62

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to cause a Denial of Service (DoS) via a crafted NAS packet. **CVE ID: CVE-2024-24423**		
Out-of-bounds Read	21-Jan-2025	7.5	The Linux Foundation Magma <= 1.8.0 (fixed in v1.9 commit 08472ba98b8321f802e95f5622fa90fec2dea486) was discovered to contain a buffer overflow in the decode_protocol_configuration_options function at /3gpp/3gpp_24.008_sm_ies.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted NAS packet. **CVE ID: CVE-2024-24417**	N/A	A-LIN-MAGM-040225/63
NULL Pointer Dereference	21-Jan-2025	6.5	A Null pointer dereference vulnerability in the Mobile Management Entity (MME) in Magma <= 1.8.0 (fixed in v1.9 commit 08472ba98b8321f802e95f5622fa90fec2dea486) allows network-adjacent attackers to crash the MME via an S1AP `Initial UE Message` packet missing an expected `EUTRAN_CGI` field. **CVE ID: CVE-2023-37033**	N/A	A-LIN-MAGM-040225/64
NULL Pointer Dereference	21-Jan-2025	6.5	A Null pointer dereference vulnerability in the Mobile Management Entity (MME) in Magma <= 1.8.0 (fixed in v1.9 commit 08472ba98b8321f802e95f5622fa90fec2dea486) allows network-adjacent attackers to crash the MME via an S1AP `Initial UE Message` packet missing an expected `TAI` field. **CVE ID: CVE-2023-37034**	N/A	A-LIN-MAGM-040225/65

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	21-Jan-2025	6.5	A Null pointer dereference vulnerability in the Mobile Management Entity (MME) in Magma <= 1.8.0 (fixed in v1.9 commit 08472ba98b8321f802e95f5622fa90fec2dea486) allows network-adjacent attackers to crash the MME via an S1AP `Uplink NAS Transport` packet missing an expected `ENB_UE_S1AP_ID` field. **CVE ID: CVE-2023-37036**	N/A	A-LIN-MAGM-040225/66
NULL Pointer Dereference	21-Jan-2025	6.5	A Null pointer dereference vulnerability in the Mobile Management Entity (MME) in Magma <= 1.8.0 (fixed in v1.9 commit 08472ba98b8321f802e95f5622fa90fec2dea486) allows network-adjacent attackers to crash the MME via an S1AP `S1Setup Request` packet missing an expected `Supported TAs` field. **CVE ID: CVE-2023-37037**	N/A	A-LIN-MAGM-040225/67
NULL Pointer Dereference	21-Jan-2025	6.5	A Null pointer dereference vulnerability in the Mobile Management Entity (MME) in Magma <= 1.8.0 (fixed in v1.9 commit 08472ba98b8321f802e95f5622fa90fec2dea486) allows network-adjacent attackers to crash the MME via an S1AP `Uplink NAS Transport` packet missing an expected `MME_UE_S1AP_ID` field. **CVE ID: CVE-2023-37038**	N/A	A-LIN-MAGM-040225/68
NULL Pointer Dereference	21-Jan-2025	6.5	A Null pointer dereference vulnerability in the Mobile Management Entity (MME) in Magma <= 1.8.0 (fixed in v1.9 commit 08472ba98b8321f802e95f	N/A	A-LIN-MAGM-040225/69

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5622fa90fec2dea486) allows network-adjacent attackers to crash the MME via an S1AP `Initial UE Message` packet missing an expected `eNB_UE_S1AP_ID` field. **CVE ID: CVE-2023-37030**		
NULL Pointer Dereference	21-Jan-2025	6.5	A Null pointer dereference vulnerability in the Mobile Management Entity (MME) in Magma <= 1.8.0 (fixed in v1.9 commit 08472ba98b8321f802e95f5622fa90fec2dea486) allows network-adjacent attackers to crash the MME via an S1AP `eNB Configuration Transfer` packet missing its required `Target eNB ID` field. **CVE ID: CVE-2023-37031**	N/A	A-LIN-MAGM-040225/70
Vendor: modalsurvey					
Product: wordpress_survey_and_poll					
Affected Version(s): * Up to (including) 1.7.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-Jan-2025	6.5	The WordPress Survey & Poll – Quiz, Survey and Poll Plugin for WordPress plugin for WordPress is vulnerable to SQL Injection via the 'id' attribute of the 'survey' shortcode in all versions up to, and including, 1.7.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with 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.	https://plugins.trac.wordpress.org/browser/wp-survey-and-poll/trunk/wordpress-survey-and-poll.php#L1457	A-MOD-WORD-040225/71

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-13596		
Vendor: open5gs					
Product: open5gs					
Affected Version(s): * Up to (including) 2.6.4					
Reachable Assertion	21-Jan-2025	7.5	A reachable assertion in the amf_ue_set_suci function of Open5GS <= 2.6.4 allows attackers to cause a Denial of Service (DoS) via a crafted NAS packet. **CVE ID: CVE-2024-24427**	N/A	A-OPE-OPEN-040225/72
Reachable Assertion	21-Jan-2025	7.5	A reachable assertion in the oai_nas_5gmm_decode function of Open5GS <= 2.6.4 allows attackers to cause a Denial of Service (DoS) via a crafted NGAP packet. **CVE ID: CVE-2024-24428**	N/A	A-OPE-OPEN-040225/73
Vendor: openimageio					
Product: openimageio					
Affected Version(s): 3.1.0.0					
Out-of-bounds Write	23-Jan-2025	9.8	OpenImageIO v3.1.0.0dev was discovered to contain a heap overflow via the component OpenImageIO_v3_1_0::farmhash::inlined::Fetch64(char const*). **CVE ID: CVE-2024-55192**	N/A	A-OPE-OPEN-040225/74
N/A	23-Jan-2025	9.8	OpenImageIO v3.1.0.0dev was discovered to contain a segmentation violation via the component /OpenImageIO/string_view.h. **CVE ID: CVE-2024-55193**	N/A	A-OPE-OPEN-040225/75
Out-of-bounds Write	23-Jan-2025	9.8	OpenImageIO v3.1.0.0dev was discovered to contain a heap overflow via the component /OpenImageIO/fmath.h.	N/A	A-OPE-OPEN-040225/76

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-55194		
Vendor: partitionnumerique					
Product: music_sheet_viewer					
Affected Version(s): * Up to (including) 4.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	30-Jan-2025	7.5	The Music Sheet Viewer plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to, and including, 4.1 via the read_score_file() function. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. **CVE ID: CVE-2024-13671**	https://plugins.trac.wordpress.org/browser/music-sheet-viewer/trunk/music-sheet-viewer.php#L748	A-PAR-MUSI-040225/77
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Jan-2025	6.4	The Music Sheet Viewer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'pn_msv' shortcode in all versions up to, and including, 4.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-13670**	https://plugins.trac.wordpress.org/browser/music-sheet-viewer/trunk/music-sheet-viewer.php#L395	A-PAR-MUSI-040225/78
Vendor: philantro					
Product: philantro					
Affected Version(s): * Up to (excluding) 5.4					
Improper Neutralization of Input During Web Page Generation	28-Jan-2025	6.4	The Philantro – Donations and Donor Management plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcodes like	https://plugins.trac.wordpress.org/changeset/3224699	A-PHI-PHIL-040225/79

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			'donate' in all versions up to, and including, 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. **CVE ID: CVE-2024-13527**		
Vendor: pluginus					
Product: meta_data_and_taxonomies_filter					
Affected Version(s): * Up to (excluding) 1.3.3.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2025	6.4	The MDTF – Meta Data and Taxonomies Filter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'mdf_results_by_ajax' shortcode in all versions up to, and including, 1.3.3.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-13340**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3224186%40wp-meta-data-filter-and-taxonomy-filter&new=3224186%40wp-meta-data-filter-and-taxonomy-filter&sfp_email=&sfph_mail=	A-PLU-META-040225/80
Vendor: projectworlds					
Product: online_food_ordering_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command	23-Jan-2025	9.8	A SQL Injection vulnerability exists in the login form of Online Food Ordering System v1.0. The vulnerability arises because the input fields	N/A	A-PRO-ONLI-040225/81

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			username and password are not properly sanitized, allowing attackers to inject malicious SQL queries to bypass authentication and gain unauthorized access. **CVE ID: CVE-2024-57328**		
Vendor: proxymis					
Product: html5_chat					
Affected Version(s): * Up to (including) 1.04					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Jan-2025	6.4	The HTML5 chat plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'HTML5CHAT' shortcode in all versions up to, and including, 1.04 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. **CVE ID: CVE-2024-12451**	https://plugins.trac.wordpress.org/browser/html5-chat/trunk/index.php#L159	A-PRO-HTML-040225/82
Vendor: quantumcloud					
Product: wpot					
Affected Version(s): * Up to (excluding) 13.5.6					
Missing Authorization	22-Jan-2025	4.3	The WPBot Pro Wordpress Chatbot plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'qc_wp_latest_update_check_pro' function in all versions up to, and including, 13.5.5. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create	N/A	A-QUA-WPOT-040225/83

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Simple Text Responses to chat queries. **CVE ID: CVE-2024-12879**		
Vendor: scriptsbundle					
Product: adforest					
Affected Version(s): * Up to (excluding) 5.1.9					
Authentication Bypass Using an Alternate Path or Channel	22-Jan-2025	9.8	The AdForest theme for WordPress is vulnerable to authentication bypass in all versions up to, and including, 5.1.8. This is due to the plugin not properly verifying a user's identity prior to logging them in as that user. This makes it possible for unauthenticated attackers to authenticate as any user as long as they have configured OTP login by phone number. **CVE ID: CVE-2024-12857**	N/A	A-SCR-ADFO-040225/84
Vendor: seventhqueen					
Product: typer_core					
Affected Version(s): * Up to (including) 1.9.6					
Authorization Bypass Through User-Controlled Key	30-Jan-2025	4.3	The Typer Core plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.9.6 via the 'elementor-template' shortcode due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from private or draft posts created by Elementor that they should not have access to. **CVE ID: CVE-2024-12102**	N/A	A-SEV-TYPE-040225/85

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: shoalsummitsolutions					
Product: team_rosters					
Affected Version(s): * Up to (including) 4.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Jan-2025	6.1	The Team Rosters plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in all versions up to, and including, 4.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-12320**	N/A	A-SHO-TEAM-040225/86
Vendor: Sonicwall					
Product: sma8200v					
Affected Version(s): * Up to (excluding) 12.4.3-02854					
Deserialization of Untrusted Data	23-Jan-2025	9.8	Pre-authentication deserialization of untrusted data vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC), which in specific conditions could potentially enable a remote unauthenticated attacker to execute arbitrary OS commands. **CVE ID: CVE-2025-23006**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002	A-SON-SMA8-040225/87
Vendor: stageshow_project					
Product: stageshow					
Affected Version(s): * Up to (including) 9.8.6					
Improper Neutralization of Input During	30-Jan-2025	6.1	The StageShow plugin for WordPress is vulnerable to Reflected Cross-Site	https://plugins.trac.wordpress.org/browser/sta	A-STA-STAG-040225/88

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Scripting due to the use of remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 9.8.6. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-13705**	geshow/trunk/admin/stageshow_manage_seating.php#L502	
Vendor: stockdio					
Product: stockdio_historical_chart					
Affected Version(s): * Up to (excluding) 2.8.19					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Jan-2025	6.4	The Stockdio Historical Chart plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'stockdio-historical-chart' shortcode in all versions up to, and including, 2.8.18 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-13349**	https://plugins.trac.wordpress.org/browser/stockdio-historical-chart/trunk/stockdioplugin.php#L1155	A-STO-STOC-040225/89
Vendor: tainacan					
Product: tainacan					
Affected Version(s): * Up to (excluding) 0.21.13					
Improper Neutralization of Special Elements used in an SQL Command	23-Jan-2025	6.5	The Tainacan plugin for WordPress is vulnerable to SQL Injection via the 'collection_id' parameter in all versions up to, and including, 0.21.12 due to	https://plugins.trac.wordpress.org/changeset/3226475/tainacan/trunk/classes/api/endpoints/	A-TAI-TAIN-040225/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID: CVE-2024-13236**	class-tainacan-rest-reports-controller.php	
Vendor: Theeventscalendar					
Product: the_events_calendar					
Affected Version(s): * Up to (excluding) 6.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2025	6.4	The The Events Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Event Calendar Link Widget through the html_tag attribute in all versions up to, and including, 6.9.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-12118**	https://plugins.trac.wordpress.org/changeset/3227009/the-events-calendar/tags/6.9.1/src/views/integrations/elementor/widgets/event-calendar-link.php	A-THE-THE_-040225/91
Vendor: themerex					
Product: addons					
Affected Version(s): * Up to (excluding) 2.34.0					
Unrestricted Upload of File with Dangerous Type	28-Jan-2025	9.8	The ThemeREX Addons plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the	N/A	A-THE-ADDO-040225/92

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			'trx_addons_uploads_save_data' function in all versions up to, and including, 2.32.3. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. **CVE ID: CVE-2024-13448**		
Vendor: themify					
Product: themify_builder					
Affected Version(s): * Up to (excluding) 7.6.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jan-2025	6.1	The Themify Builder plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 7.6.5. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-13319**	https://plugins.trac.wordpress.org/changeset/3224684/themify-builder/trunk/themify/themify-admin.php	A-THE-THEM-040225/93
Vendor: thimpress					
Product: wp_hotel_booking					
Affected Version(s): * Up to (excluding) 2.1.7					
Missing Authorization	22-Jan-2025	4.3	The WP Hotel Booking plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the hotel_booking_load_order_user AJAX action in all versions up to, and including, 2.1.6. This makes it possible for authenticated attackers,	https://plugins.trac.wordpress.org/changeset/3225879/	A-THI-WP_H-040225/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with Subscriber-level access and above, to retrieve a list of registered user emails. **CVE ID: CVE-2024-13447**		
Vendor: Videowhisper					
Product: broadcast_live_video					
Affected Version(s): * Up to (excluding) 6.1.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2025	6.4	The Broadcast Live Video – Live Streaming : HTML5, WebRTC, HLS, RTSP, RTMP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'videowhisper_hls' shortcode in all versions up to, and including, 6.1.9 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. **CVE ID: CVE-2024-12504**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3218331%40videowhisper-live-streaming-integration&new=3218331%40videowhisper-live-streaming-integration&sfp_email=&sfph_mail=	A-VID-BROA-040225/95
Product: picture_gallery					
Affected Version(s): * Up to (excluding) 1.5.20					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jan-2025	6.4	The Picture Gallery – Frontend Image Uploads, AJAX Photo List plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'videowhisper_pictures' shortcode in all versions up to, and including, 1.5.19 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3218329%40picture-gallery&new=3218329%40picture-gallery&sfp_email=&sfph_mail=	A-VID-PICT-040225/96

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-13584**		
Vendor: villatheme					
Product: w2s					
Affected Version(s): * Up to (excluding) 1.3.0					
External Control of File Name or Path	30-Jan-2025	6.5	The W2S – Migrate WooCommerce to Shopify plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to, and including, 1.2.1 via the 'viw2s_view_log' AJAX action. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information. **CVE ID: CVE-2024-12861**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3227799%40w2s-migrate-woo-to-shopify&new=3227799%40w2s-migrate-woo-to-shopify&sfp_email=&sfph_mail=	A-VIL-W2S-040225/97
Vendor: vinayjain					
Product: embed_swagger_ui					
Affected Version(s): * Up to (including) 1.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Jan-2025	6.4	The Embed Swagger UI plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wpsgui' shortcode in all versions up to, and including, 1.0.0 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.	N/A	A-VIN-EMBE-040225/98

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-13700		
Vendor: visualmodo					
Product: borderless					
Affected Version(s): * Up to (including) 1.5.9					
Improper Control of Generation of Code ('Code Injection')	30-Jan-2025	7.2	The Borderless – Widgets, Elements, Templates and Toolkit for Elementor & Gutenberg plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.5.9 via the 'write_config' function. This is due to a lack of sanitization on an imported JSON file. This makes it possible for authenticated attackers, with Administrator-level access and above, to execute code on the server. **CVE ID: CVE-2024-11600**	https://plugins.trac.wordpress.org/browser/borderless/tags/1.5.7/includes/icon-manager/icon-manager.php#L249, https://plugins.trac.wordpress.org/browser/borderless/tags/1.5.7/includes/icon-manager/icon-manager.php#L333	A-VIS-BORD-040225/99
Missing Authorization	30-Jan-2025	4.3	The Borderless – Widgets, Elements, Templates and Toolkit for Elementor & Gutenberg plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'remove_zipped_font' function in all versions up to, and including, 1.5.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete icon fonts that were previously uploaded. **CVE ID: CVE-2024-11583**	N/A	A-VIS-BORD-040225/100
Vendor: vruiz					
Product: vr-frases					
Affected Version(s): * Up to (including) 3.0.1					
Improper Neutralization	30-Jan-2025	6.1	The VR-Frases (collect & share quotes) plugin for	https://plugins.svn.wordpress.o	A-VRU-VR-F-040225/101

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Input During Web Page Generation ('Cross-site Scripting')			WordPress is vulnerable to Reflected Cross-Site Scripting via several parameters in all versions up to, and including, 3.0.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2025-0860**	rg/vr-frases/tags/3.0.1/includes/vr-frases-admin.php	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-Jan-2025	4.9	The VR-Frases (collect & share quotes) plugin for WordPress is vulnerable to SQL Injection via several parameters in all versions up to, and including, 3.0.1 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. **CVE ID: CVE-2025-0861**	https://plugins.svn.wordpress.org/vr-frases/tags/3.0.1/includes/vr-frases-admin.php	A-VRU-VR-F-040225/102
Vendor: wallosapp					
Product: wallos					
Affected Version(s): 2.41.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2025	6.1	Cross Site Scripting vulnerability in Wallos v.2.41.0 allows a remote attacker to execute arbitrary code via the profile picture function.	N/A	A-WAL-WALL-040225/103

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-57386		
Vendor: westguardsolutions					
Product: ws_form					
Affected Version(s): * Up to (excluding) 1.10.14					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jan-2025	7.2	The WS Form LITE – Drag & Drop Contact Form Builder for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the url parameter in all versions up to, and including, 1.10.13 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. NOTE: This vulnerability is partially fixed in 1.10.13 and completely fixed in 1.10.14. **CVE ID: CVE-2024-13509**	https://plugins.trac.wordpress.org/changeset/3225862/ws-form, https://plugins.trac.wordpress.org/changeset/3226595/ws-form	A-WES-WS_F-040225/104
Vendor: wonderjarcreative					
Product: wonder_fontawesome					
Affected Version(s): * Up to (including) 0.8					
Cross-Site Request Forgery (CSRF)	30-Jan-2025	6.1	The Wonder FontAwesome plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.8. This is due to missing or incorrect nonce validation on one of its functions. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into	N/A	A-WON-WOND-040225/105

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			performing an action such as clicking on a link. **CVE ID: CVE-2024-13512**		
Vendor: wordpresteem					
Product: we_-_testimonial_slide					
Affected Version(s): * Up to (including) 1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Jan-2025	6.4	The WE – Testimonial Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Testimonial Author Names in all versions up to, and including, 1.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-13460**	N/A	A-WOR-WE_--040225/106
Vendor: wp-polls_project					
Product: wp-polls					
Affected Version(s): * Up to (excluding) 2.77.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Jan-2025	5.4	The WP-Polls plugin for WordPress is vulnerable to SQL Injection via COOKIE in all versions up to, and including, 2.77.2 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. Those queries are stored and results are not displayed to the attacker, which means	https://github.com/WordPress/wordpress-develop/blob/a82874058f58575dbba64ce09b6dcbd43ccf5fdc/src/wp-includes/default-constants.php#L249, https://github.com/lesterchan/wp-polls/blob/97ab44c2d4c3a3d308ce8b87dae8b2	A-WP--WP-P-040225/107

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			they cannot be exploited to obtain any additional information about the database. However, a properly configured payload allows for the injection of malicious JavaScript resulting in Stored Cross-Site Scripting. **CVE ID: CVE-2024-13426**	a8f7147f0e/polls-logs.php#L294	
Vendor: wpbean					
Product: wp_post_list_table					
Affected Version(s): * Up to (excluding) 1.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Jan-2025	6.4	The WP Post List Table plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wpb_post_list_table' shortcode in all versions up to, and including, 1.0.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-13664**	https://plugins.trac.wordpress.org/changeset/3227735/	A-WPB-WP_P-040225/108
Vendor: wpbot					
Product: wpot					
Affected Version(s): * Up to (excluding) 13.5.6					
Unrestricted Upload of File with Dangerous Type	22-Jan-2025	9.8	The WPBot Pro Wordpress Chatbot plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'qcld_wpcfb_file_upload' function in all versions up to, and including, 13.5.4. This makes it possible for	N/A	A-WPB-WPOT-040225/109

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. Note: The exploit requires thee ChatBot Conversational Forms plugin and the Conversational Form Builder Pro addon plugin. **CVE ID: CVE-2024-13091**		
Vendor: wpdispensary					
Product: wp_dispensary					
Affected Version(s): * Up to (including) 4.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Jan-2025	6.4	The WP Dispensary plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wpd_menu' shortcode in all versions up to, and including, 4.5.0 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. **CVE ID: CVE-2024-12444**	N/A	A-WPD-WP_D-040225/110
Vendor: wpmessiah					
Product: ai_image_alt_text_generator_for_wp					
Affected Version(s): * Up to (excluding) 1.0.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Jan-2025	6.1	The Ai Image Alt Text Generator for WP plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'page' parameter in all versions up to, and including, 1.0.2 due to insufficient input sanitization and output	N/A	A-WPM-AI_I-040225/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-12177**		
Product: safe_ai_malware_protection_for_wp					
Affected Version(s): * Up to (including) 1.0.17					
Missing Authorization	30-Jan-2025	7.5	The Safe Ai Malware Protection for WP plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the export_db() function in all versions up to, and including, 1.0.17. This makes it possible for unauthenticated attackers to retrieve a complete dump of the site's database. **CVE ID: CVE-2024-12269**	https://plugins.trac.wordpress.org/browser/safe-ai-malware-protection-for-wp/trunk/includes/class-mvsp-export-db.php#L7	A-WPM-SAFE-040225/112
Vendor: wpmet					
Product: elementskit					
Affected Version(s): * Up to (excluding) 3.7.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jan-2025	6.4	The ElementsKit Pro plugin for WordPress is vulnerable to DOM-Based Stored Cross-Site Scripting via the 'url' parameter in all versions up to, and including, 3.7.8 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	N/A	A-WPM-ELEM-040225/113

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			whenever a user accesses an injected page. **CVE ID: CVE-2025-0321**		
Vendor: wptableeditor					
Product: table_editor					
Affected Version(s): * Up to (excluding) 1.6.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Jan-2025	6.4	The Table Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wptableeditor_vtabs' shortcode in all versions up to, and including, 1.5.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-13661**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3228279%40wp-table-editor&new=3228279%40wp-table-editor&sfp_email=&sfph_mail=	A-WPT-TABL-040225/114
Vendor: ylefebvre					
Product: link_library					
Affected Version(s): * Up to (excluding) 7.7.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jan-2025	6.1	The Link Library plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'searchll' parameter in all versions up to, and including, 7.7.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3225694%40link-library&new=3225694%40link-library&sfp_email=&sfph_mail=	A-YLE-LINK-040225/115

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-13404		
Hardware					
Vendor: Sonicwall					
Product: sma6200					
Affected Version(s): -					
Deserialization of Untrusted Data	23-Jan-2025	9.8	Pre-authentication deserialization of untrusted data vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC), which in specific conditions could potentially enable a remote unauthenticated attacker to execute arbitrary OS commands. **CVE ID: CVE-2025-23006**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002	H-SON-SMA6-040225/116
Product: sma6210					
Affected Version(s): -					
Deserialization of Untrusted Data	23-Jan-2025	9.8	Pre-authentication deserialization of untrusted data vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC), which in specific conditions could potentially enable a remote unauthenticated attacker to execute arbitrary OS commands. **CVE ID: CVE-2025-23006**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002	H-SON-SMA6-040225/117
Product: sma7200					
Affected Version(s): -					
Deserialization of Untrusted Data	23-Jan-2025	9.8	Pre-authentication deserialization of untrusted data vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) and Central	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002	H-SON-SMA7-040225/118

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management Console (CMC), which in specific conditions could potentially enable a remote unauthenticated attacker to execute arbitrary OS commands. **CVE ID: CVE-2025-23006**		
Product: sma7210					
Affected Version(s): -					
Deserialization of Untrusted Data	23-Jan-2025	9.8	Pre-authentication deserialization of untrusted data vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC), which in specific conditions could potentially enable a remote unauthenticated attacker to execute arbitrary OS commands. **CVE ID: CVE-2025-23006**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002	H-SON-SMA7-040225/119
Product: sra_ex6000					
Affected Version(s): -					
Deserialization of Untrusted Data	23-Jan-2025	9.8	Pre-authentication deserialization of untrusted data vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC), which in specific conditions could potentially enable a remote unauthenticated attacker to execute arbitrary OS commands. **CVE ID: CVE-2025-23006**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002	H-SON-SRA_-040225/120
Product: sra_ex7000					
Affected Version(s): -					
Deserialization of Untrusted Data	23-Jan-2025	9.8	Pre-authentication deserialization of untrusted data vulnerability has been	https://psirt.global.sonicwall.com/vuln-	H-SON-SRA_-040225/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identified in the SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC), which in specific conditions could potentially enable a remote unauthenticated attacker to execute arbitrary OS commands. **CVE ID: CVE-2025-23006**	detail/SNWLID-2025-0002	
Product: sra_ex9000					
Affected Version(s): -					
Deserialization of Untrusted Data	23-Jan-2025	9.8	Pre-authentication deserialization of untrusted data vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC), which in specific conditions could potentially enable a remote unauthenticated attacker to execute arbitrary OS commands. **CVE ID: CVE-2025-23006**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002	H-SON-SRA_-040225/122
Vendor: Tenda					
Product: ac18					
Affected Version(s): -					
Out-of-bounds Write	16-Jan-2025	9.8	Tenda AC18 V15.03.05.19 was discovered to contain a stack overflow via the ssid parameter in the form_fast_setting_wifi_set function. **CVE ID: CVE-2024-57575**	N/A	H-TEN-AC18-040225/123
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Jan-2025	9.8	Tenda AC18 V15.03.05.19 was discovered to contain a command injection vulnerability via the usbName parameter in the formSetSambaConf function.	N/A	H-TEN-AC18-040225/124

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-57583		
Operating System					
Vendor: Apple					
Product: ipados					
Affected Version(s): * Up to (excluding) 17.7.3					
N/A	27-Jan-2025	5.3	A logic issue was addressed with improved file handling. This issue is fixed in macOS Ventura 13.7.2, iOS 18.2 and iPadOS 18.2, iPadOS 17.7.3, macOS Sonoma 14.7.2, macOS Sequoia 15.2. Photos in the Hidden Photos Album may be viewed without authentication. **CVE ID: CVE-2024-54488**	N/A	O-APP-IPAD-040225/125
Affected Version(s): * Up to (excluding) 17.7.4					
N/A	27-Jan-2025	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.2, tvOS 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sequoia 15.2. Processing web content may lead to a denial-of-service. **CVE ID: CVE-2024-54497**	N/A	O-APP-IPAD-040225/126
N/A	27-Jan-2025	5.5	The issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. Processing an image may lead to a denial-of-service. **CVE ID: CVE-2025-24086**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-	O-APP-IPAD-040225/127

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/122070, https://support.apple.com/en-us/122071	
Improper Link Resolution Before File Access ('Link Following')	27-Jan-2025	5.5	This issue was addressed with improved handling of symlinks. This issue is fixed in iPadOS 17.7.4, iOS 18.3 and iPadOS 18.3. Restoring a maliciously crafted backup file may lead to modification of protected system files. **CVE ID: CVE-2025-24104**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067	O-APP-IPAD-040225/128
N/A	27-Jan-2025	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, tvOS 18.3. Parsing a file may lead to an unexpected app termination. **CVE ID: CVE-2025-24127**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070, https://support.apple.com/en-us/122072	O-APP-IPAD-040225/129
Insecure Storage of Sensitive Information	27-Jan-2025	5.5	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iPadOS 17.7.4, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3. An app may be able to fingerprint the user. **CVE ID: CVE-2025-24117**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122073	O-APP-IPAD-040225/130
N/A	27-Jan-2025	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS	https://support.apple.com/en-us/122066,	O-APP-IPAD-040225/131

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			17.7.4, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. Parsing a file may lead to an unexpected app termination. **CVE ID: CVE-2025-24161**	https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072	
Affected Version(s): * Up to (excluding) 18.2					
N/A	27-Jan-2025	9.1	The issue was addressed by removing the relevant flags. This issue is fixed in watchOS 11.2, iOS 18.2 and iPadOS 18.2. A system binary could be used to fingerprint a user's Apple Account. **CVE ID: CVE-2024-54512**	N/A	O-APP-IPAD-040225/132
Out-of-bounds Write	27-Jan-2025	8.8	The issue was addressed with improved memory handling. This issue is fixed in visionOS 2.2, tvOS 18.2, Safari 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sequoia 15.2. Processing maliciously crafted web content may lead to memory corruption. **CVE ID: CVE-2024-54543**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845, https://support.apple.com/en-us/121846	O-APP-IPAD-040225/133
Out-of-bounds Write	27-Jan-2025	7.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sequoia 15.2, watchOS 11.2, tvOS 18.2, iOS 18.2 and iPadOS 18.2. An app may be able to	N/A	O-APP-IPAD-040225/134

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			corrupt coprocessor memory. **CVE ID: CVE-2024-54522**		
Out-of-bounds Write	27-Jan-2025	7.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sequoia 15.2, watchOS 11.2, tvOS 18.2, iOS 18.2 and iPadOS 18.2. An app may be able to corrupt coprocessor memory. **CVE ID: CVE-2024-54517**	N/A	O-APP-IPAD-040225/135
N/A	27-Jan-2025	5.5	This issue was addressed through improved state management. This issue is fixed in macOS Ventura 13.7.2, visionOS 2.2, tvOS 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sonoma 14.7.2, macOS Sequoia 15.2. An app may be able to access user-sensitive data. **CVE ID: CVE-2024-54541**	N/A	O-APP-IPAD-040225/136
Affected Version(s): * Up to (excluding) 18.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Jan-2025	8.8	A privacy issue was addressed with improved handling of files. This issue is fixed in macOS Sequoia 15.3, Safari 18.3, iOS 18.3 and iPadOS 18.3. Copying a URL from Web Inspector may lead to command injection. **CVE ID: CVE-2025-24150**	N/A	O-APP-IPAD-040225/137
N/A	27-Jan-2025	7.8	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.3, tvOS 18.3, watchOS 11.3, iOS 18.3 and iPadOS 18.3. A malicious app may be able to gain root privileges.	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.	O-APP-IPAD-040225/138

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-24107	apple.com/en-us/122072	
Use After Free	27-Jan-2025	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. A malicious application may be able to elevate privileges. Apple is aware of a report that this issue may have been actively exploited against versions of iOS before iOS 17.2. **CVE ID: CVE-2025-24085**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072, https://support.apple.com/en-us/122073	O-APP-IPAD-040225/139
NULL Pointer Dereference	27-Jan-2025	7.5	A null pointer dereference was addressed with improved input validation. This issue is fixed in macOS Sequoia 15.3, iOS 18.3 and iPadOS 18.3. A remote attacker may be able to cause a denial-of-service. **CVE ID: CVE-2025-24177**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068	O-APP-IPAD-040225/140
Access of Resource Using Incompatible Type ('Type Confusion')	27-Jan-2025	7.5	A type confusion issue was addressed with improved checks. This issue is fixed in visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. A remote attacker may cause an unexpected app termination. **CVE ID: CVE-2025-24129**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072, https://support.apple.com/en-us/122073	O-APP-IPAD-040225/141
N/A	27-Jan-2025	6.5	The issue was addressed with improved access restrictions to the file system. This issue is fixed in macOS Sequoia 15.3, Safari 18.3, iOS 18.3 and iPadOS 18.3, visionOS 2.3. A maliciously crafted	N/A	O-APP-IPAD-040225/142

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webpage may be able to fingerprint the user. **CVE ID: CVE-2025-24143**		
N/A	27-Jan-2025	6.5	The issue was addressed with improved memory handling. This issue is fixed in visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. An attacker in a privileged position may be able to perform a denial-of-service. **CVE ID: CVE-2025-24131**	N/A	O-APP-IPAD-040225/143
N/A	27-Jan-2025	4.3	The issue was addressed with improved UI. This issue is fixed in macOS Sequoia 15.3, Safari 18.3, iOS 18.3 and iPadOS 18.3, visionOS 2.3. Visiting a malicious website may lead to user interface spoofing. **CVE ID: CVE-2025-24113**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122073, https://support.apple.com/en-us/122074	O-APP-IPAD-040225/144
N/A	27-Jan-2025	4.3	The issue was addressed by adding additional logic. This issue is fixed in macOS Sequoia 15.3, Safari 18.3, iOS 18.3 and iPadOS 18.3. Visiting a malicious website may lead to address bar spoofing. **CVE ID: CVE-2025-24128**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122074	O-APP-IPAD-040225/145
Insertion of Sensitive Information into Log File	27-Jan-2025	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sequoia 15.3, iOS 18.3 and iPadOS 18.3. An app may be able to view a contact's phone number in system logs. **CVE ID: CVE-2025-24145**	N/A	O-APP-IPAD-040225/146
N/A	27-Jan-2025	3.3	An authentication issue was addressed with improved	N/A	O-APP-IPAD-040225/147

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			state management. This issue is fixed in iOS 18.3 and iPadOS 18.3. An attacker with physical access to an unlocked device may be able to access Photos while the app is locked. **CVE ID: CVE-2025-24141**		
Affected Version(s): From (including) 18.0 Up to (excluding) 18.2					
N/A	27-Jan-2025	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.2, tvOS 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sequoia 15.2. Processing web content may lead to a denial-of-service. **CVE ID: CVE-2024-54497**	N/A	O-APP-IPAD-040225/148
N/A	27-Jan-2025	5.3	A logic issue was addressed with improved file handling. This issue is fixed in macOS Ventura 13.7.2, iOS 18.2 and iPadOS 18.2, iPadOS 17.7.3, macOS Sonoma 14.7.2, macOS Sequoia 15.2. Photos in the Hidden Photos Album may be viewed without authentication. **CVE ID: CVE-2024-54488**	N/A	O-APP-IPAD-040225/149
Affected Version(s): From (including) 18.0 Up to (excluding) 18.3					
N/A	27-Jan-2025	5.5	The issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. Processing an image may lead to a denial-of-service.	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069,	O-APP-IPAD-040225/150

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-24086	https://support.apple.com/en-us/122070, https://support.apple.com/en-us/122071	
Improper Link Resolution Before File Access ('Link Following')	27-Jan-2025	5.5	This issue was addressed with improved handling of symlinks. This issue is fixed in iPadOS 17.7.4, iOS 18.3 and iPadOS 18.3. Restoring a maliciously crafted backup file may lead to modification of protected system files. **CVE ID: CVE-2025-24104**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067	O-APP-IPAD-040225/151
N/A	27-Jan-2025	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, tvOS 18.3. Parsing a file may lead to an unexpected app termination. **CVE ID: CVE-2025-24127**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070, https://support.apple.com/en-us/122072	O-APP-IPAD-040225/152
Insecure Storage of Sensitive Information	27-Jan-2025	5.5	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iPadOS 17.7.4, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3. An app may be able to fingerprint the user. **CVE ID: CVE-2025-24117**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122073	O-APP-IPAD-040225/153
Product: iphone_os					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 18.2					
N/A	27-Jan-2025	9.1	The issue was addressed by removing the relevant flags. This issue is fixed in watchOS 11.2, iOS 18.2 and iPadOS 18.2. A system binary could be used to fingerprint a user's Apple Account. **CVE ID: CVE-2024-54512**	N/A	O-APP-IPHO-040225/154
Out-of-bounds Write	27-Jan-2025	8.8	The issue was addressed with improved memory handling. This issue is fixed in visionOS 2.2, tvOS 18.2, Safari 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sequoia 15.2. Processing maliciously crafted web content may lead to memory corruption. **CVE ID: CVE-2024-54543**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845, https://support.apple.com/en-us/121846	O-APP-IPHO-040225/155
Out-of-bounds Write	27-Jan-2025	7.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sequoia 15.2, watchOS 11.2, tvOS 18.2, iOS 18.2 and iPadOS 18.2. An app may be able to corrupt coprocessor memory. **CVE ID: CVE-2024-54522**	N/A	O-APP-IPHO-040225/156
Out-of-bounds Write	27-Jan-2025	7.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sequoia 15.2, watchOS 11.2, tvOS 18.2, iOS 18.2 and iPadOS 18.2. An app may be able to corrupt coprocessor memory. **CVE ID: CVE-2024-54517**	N/A	O-APP-IPHO-040225/157

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	27-Jan-2025	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.2, tvOS 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sequoia 15.2. Processing web content may lead to a denial-of-service. **CVE ID: CVE-2024-54497**	N/A	O-APP-IPHO-040225/158
N/A	27-Jan-2025	5.5	This issue was addressed through improved state management. This issue is fixed in macOS Ventura 13.7.2, visionOS 2.2, tvOS 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sonoma 14.7.2, macOS Sequoia 15.2. An app may be able to access user-sensitive data. **CVE ID: CVE-2024-54541**	N/A	O-APP-IPHO-040225/159
N/A	27-Jan-2025	5.3	A logic issue was addressed with improved file handling. This issue is fixed in macOS Ventura 13.7.2, iOS 18.2 and iPadOS 18.2, iPadOS 17.7.3, macOS Sonoma 14.7.2, macOS Sequoia 15.2. Photos in the Hidden Photos Album may be viewed without authentication. **CVE ID: CVE-2024-54488**	N/A	O-APP-IPHO-040225/160
Affected Version(s): * Up to (excluding) 18.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Jan-2025	8.8	A privacy issue was addressed with improved handling of files. This issue is fixed in macOS Sequoia 15.3, Safari 18.3, iOS 18.3 and iPadOS 18.3. Copying a URL from Web Inspector may lead to command injection.	N/A	O-APP-IPHO-040225/161

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-24150		
N/A	27-Jan-2025	7.8	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.3, tvOS 18.3, watchOS 11.3, iOS 18.3 and iPadOS 18.3. A malicious app may be able to gain root privileges. **CVE ID: CVE-2025-24107**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072	O-APP-IPHO-040225/162
Use After Free	27-Jan-2025	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. A malicious application may be able to elevate privileges. Apple is aware of a report that this issue may have been actively exploited against versions of iOS before iOS 17.2. **CVE ID: CVE-2025-24085**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072, https://support.apple.com/en-us/122073	O-APP-IPHO-040225/163
Access of Resource Using Incompatible Type ('Type Confusion')	27-Jan-2025	7.5	A type confusion issue was addressed with improved checks. This issue is fixed in visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. A remote attacker may cause an unexpected app termination. **CVE ID: CVE-2025-24129**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072, https://support.apple.com/en-us/122073	O-APP-IPHO-040225/164
NULL Pointer Dereference	27-Jan-2025	7.5	A null pointer dereference was addressed with improved input validation. This issue is fixed in macOS Sequoia 15.3, iOS 18.3 and iPadOS 18.3. A remote	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068	O-APP-IPHO-040225/165

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker may be able to cause a denial-of-service. **CVE ID: CVE-2025-24177**		
N/A	27-Jan-2025	6.5	The issue was addressed with improved memory handling. This issue is fixed in visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. An attacker in a privileged position may be able to perform a denial-of-service. **CVE ID: CVE-2025-24131**	N/A	O-APP-IPHO-040225/166
N/A	27-Jan-2025	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. Parsing a file may lead to an unexpected app termination. **CVE ID: CVE-2025-24161**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072	O-APP-IPHO-040225/167
N/A	27-Jan-2025	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, tvOS 18.3. Parsing a file may lead to an unexpected app termination. **CVE ID: CVE-2025-24127**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070, https://support.	O-APP-IPHO-040225/168

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				apple.com/en-us/122072	
Insecure Storage of Sensitive Information	27-Jan-2025	5.5	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iPadOS 17.7.4, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3. An app may be able to fingerprint the user. **CVE ID: CVE-2025-24117**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122073	O-APP-IPHO-040225/169
Improper Link Resolution Before File Access ('Link Following')	27-Jan-2025	5.5	This issue was addressed with improved handling of symlinks. This issue is fixed in iPadOS 17.7.4, iOS 18.3 and iPadOS 18.3. Restoring a maliciously crafted backup file may lead to modification of protected system files. **CVE ID: CVE-2025-24104**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067	O-APP-IPHO-040225/170
N/A	27-Jan-2025	5.5	The issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. Processing an image may lead to a denial-of-service. **CVE ID: CVE-2025-24086**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070, https://support.apple.com/en-us/122071	O-APP-IPHO-040225/171
N/A	27-Jan-2025	4.3	The issue was addressed with improved UI. This issue is fixed in macOS Sequoia 15.3, Safari 18.3, iOS 18.3 and iPadOS 18.3,	https://support.apple.com/en-	O-APP-IPHO-040225/172

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			visionOS 2.3. Visiting a malicious website may lead to user interface spoofing. **CVE ID: CVE-2025-24113**	us/122068, https://support.apple.com/en-us/122073, https://support.apple.com/en-us/122074	
N/A	27-Jan-2025	4.3	The issue was addressed by adding additional logic. This issue is fixed in macOS Sequoia 15.3, Safari 18.3, iOS 18.3 and iPadOS 18.3. Visiting a malicious website may lead to address bar spoofing. **CVE ID: CVE-2025-24128**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122074	O-APP-IPHO-040225/173
Insertion of Sensitive Information into Log File	27-Jan-2025	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sequoia 15.3, iOS 18.3 and iPadOS 18.3. An app may be able to view a contact's phone number in system logs. **CVE ID: CVE-2025-24145**	N/A	O-APP-IPHO-040225/174
N/A	27-Jan-2025	3.3	An authentication issue was addressed with improved state management. This issue is fixed in iOS 18.3 and iPadOS 18.3. An attacker with physical access to an unlocked device may be able to access Photos while the app is locked. **CVE ID: CVE-2025-24141**	N/A	O-APP-IPHO-040225/175
Product: macos					
Affected Version(s): * Up to (excluding) 13.7.2					
N/A	27-Jan-2025	7.5	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Sonoma 14.7.2, macOS Sequoia 15.2, macOS Ventura 13.7.2. An attacker may gain access to protected parts of the file system.	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	O-APP-MACO-040225/176

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-54557		
N/A	27-Jan-2025	5.5	This issue was addressed through improved state management. This issue is fixed in macOS Ventura 13.7.2, visionOS 2.2, tvOS 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sonoma 14.7.2, macOS Sequoia 15.2. An app may be able to access user-sensitive data. **CVE ID: CVE-2024-54541**	N/A	O-APP-MACO-040225/177
N/A	27-Jan-2025	5.3	A logic issue was addressed with improved file handling. This issue is fixed in macOS Ventura 13.7.2, iOS 18.2 and iPadOS 18.2, iPadOS 17.7.3, macOS Sonoma 14.7.2, macOS Sequoia 15.2. Photos in the Hidden Photos Album may be viewed without authentication. **CVE ID: CVE-2024-54488**	N/A	O-APP-MACO-040225/178
Affected Version(s): * Up to (excluding) 13.7.3					
Integer Overflow or Wraparound	27-Jan-2025	7.8	An integer overflow was addressed through improved input validation. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. An app may be able to elevate privileges. **CVE ID: CVE-2025-24156**	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070	O-APP-MACO-040225/179
N/A	27-Jan-2025	7.5	This issue was addressed by improved management of object lifetimes. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. An attacker may be able to cause unexpected app termination.	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070	O-APP-MACO-040225/180

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-24120		
N/A	27-Jan-2025	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.2, tvOS 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sequoia 15.2. Processing web content may lead to a denial-of-service. **CVE ID: CVE-2024-54497**	N/A	O-APP-MACO-040225/181
N/A	27-Jan-2025	5.5	The issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. Processing an image may lead to a denial-of-service. **CVE ID: CVE-2025-24086**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070, https://support.apple.com/en-us/122071	O-APP-MACO-040225/182
N/A	27-Jan-2025	5.5	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. An app may be able to modify protected parts of the file system. **CVE ID: CVE-2025-24114**	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070	O-APP-MACO-040225/183
N/A	27-Jan-2025	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.3, iOS	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067,	O-APP-MACO-040225/184

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			18.3 and iPadOS 18.3, macOS Sequoia 15.3, tvOS 18.3. Parsing a file may lead to an unexpected app termination. **CVE ID: CVE-2025-24127**	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070, https://support.apple.com/en-us/122072	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	27-Jan-2025	4.7	A race condition was addressed with additional validation. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. An app may be able to access user-sensitive data. **CVE ID: CVE-2025-24094**	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070	O-APP-MACO-040225/185
N/A	27-Jan-2025	4.4	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. An app may be able to bypass Privacy preferences. **CVE ID: CVE-2025-24116**	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070	O-APP-MACO-040225/186
Improper Link Resolution Before File Access ('Link Following')	27-Jan-2025	4.4	This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. A malicious app may be able to create symlinks to protected regions of the disk. **CVE ID: CVE-2025-24136**	N/A	O-APP-MACO-040225/187
N/A	27-Jan-2025	3.3	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. An app may be able to access	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.	O-APP-MACO-040225/188

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about a user's contacts. **CVE ID: CVE-2025-24100**	apple.com/en-us/122070	
N/A	27-Jan-2025	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.7.3, macOS Sonoma 14.7.3, macOS Sequoia 15. An app may be able to access contacts. **CVE ID: CVE-2024-44172**	N/A	O-APP-MACO-040225/189
Affected Version(s): * Up to (excluding) 14.7.2					
Out-of-bounds Write	27-Jan-2025	7.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Sonoma 14.7.2, macOS Sequoia 15.2, macOS Sonoma 14.7.3. An app may be able to cause unexpected system termination or write kernel memory. **CVE ID: CVE-2024-54509**	N/A	O-APP-MACO-040225/190
N/A	27-Jan-2025	3.3	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.7.2, macOS Sequoia 15.2. An app may be able to approve a launch daemon without user consent. **CVE ID: CVE-2024-54516**	N/A	O-APP-MACO-040225/191
Affected Version(s): * Up to (excluding) 14.7.3					
N/A	27-Jan-2025	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.3, macOS Sonoma 14.7.3. Parsing a file may lead to an unexpected app termination. **CVE ID: CVE-2025-24112**	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069	O-APP-MACO-040225/192

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	27-Jan-2025	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. Parsing a file may lead to an unexpected app termination. **CVE ID: CVE-2025-24161**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072	O-APP-MACO-040225/193
Affected Version(s): * Up to (excluding) 15.2					
Out-of-bounds Write	27-Jan-2025	8.8	The issue was addressed with improved memory handling. This issue is fixed in visionOS 2.2, tvOS 18.2, Safari 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sequoia 15.2. Processing maliciously crafted web content may lead to memory corruption. **CVE ID: CVE-2024-54543**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845, https://support.apple.com/en-us/121846	O-APP-MACO-040225/194
Out-of-bounds Write	27-Jan-2025	7.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sequoia 15.2, watchOS 11.2, tvOS 18.2, iOS 18.2 and iPadOS 18.2. An app may be able to corrupt coprocessor memory. **CVE ID: CVE-2024-54517**	N/A	O-APP-MACO-040225/195
Out-of-bounds Write	27-Jan-2025	7.8	The issue was addressed with improved bounds checks. This issue is fixed in	N/A	O-APP-MACO-040225/196

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Sequoia 15.2, watchOS 11.2, tvOS 18.2, iOS 18.2 and iPadOS 18.2. An app may be able to corrupt coprocessor memory. **CVE ID: CVE-2024-54522**		
N/A	27-Jan-2025	5.5	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sequoia 15.2. An app may be able to access user-sensitive data. **CVE ID: CVE-2024-54549**	https://support.apple.com/en-us/121839	O-APP-MACO-040225/197
N/A	27-Jan-2025	5.5	The issue was addressed with improved validation of environment variables. This issue is fixed in macOS Sequoia 15.2. An app may be able to edit NVRAM variables. **CVE ID: CVE-2024-54536**	N/A	O-APP-MACO-040225/198
Affected Version(s): * Up to (excluding) 15.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Jan-2025	8.8	A privacy issue was addressed with improved handling of files. This issue is fixed in macOS Sequoia 15.3, Safari 18.3, iOS 18.3 and iPadOS 18.3. Copying a URL from Web Inspector may lead to command injection. **CVE ID: CVE-2025-24150**	N/A	O-APP-MACO-040225/199
N/A	27-Jan-2025	7.8	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.3, tvOS 18.3, watchOS 11.3, iOS 18.3 and iPadOS 18.3. A malicious app may be able to gain root privileges. **CVE ID: CVE-2025-24107**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072	O-APP-MACO-040225/200

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	27-Jan-2025	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. A malicious application may be able to elevate privileges. Apple is aware of a report that this issue may have been actively exploited against versions of iOS before iOS 17.2. **CVE ID: CVE-2025-24085**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072, https://support.apple.com/en-us/122073	O-APP-MACO-040225/201
Access of Resource Using Incompatible Type ('Type Confusion')	27-Jan-2025	7.5	A type confusion issue was addressed with improved checks. This issue is fixed in visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. A remote attacker may cause an unexpected app termination. **CVE ID: CVE-2025-24129**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072, https://support.apple.com/en-us/122073	O-APP-MACO-040225/202
N/A	27-Jan-2025	7.5	A logging issue was addressed with improved data redaction. This issue is fixed in macOS Sequoia 15.3, Safari 18.3. A malicious app may be able to bypass browser extension authentication. **CVE ID: CVE-2025-24169**	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122074	O-APP-MACO-040225/203
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	27-Jan-2025	6.7	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.3. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID: CVE-2025-24153**	https://support.apple.com/en-us/122068	O-APP-MACO-040225/204

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	27-Jan-2025	6.5	The issue was addressed with improved memory handling. This issue is fixed in visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. An attacker in a privileged position may be able to perform a denial-of-service. **CVE ID: CVE-2025-24131**	N/A	O-APP-MACO-040225/205
N/A	27-Jan-2025	6.5	The issue was addressed with improved access restrictions to the file system. This issue is fixed in macOS Sequoia 15.3, Safari 18.3, iOS 18.3 and iPadOS 18.3, visionOS 2.3. A maliciously crafted webpage may be able to fingerprint the user. **CVE ID: CVE-2025-24143**	N/A	O-APP-MACO-040225/206
N/A	27-Jan-2025	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.3. An app may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID: CVE-2025-24152**	https://support.apple.com/en-us/122068	O-APP-MACO-040225/207
Insecure Storage of Sensitive Information	27-Jan-2025	5.5	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iPadOS 17.7.4, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3. An app may be able to fingerprint the user. **CVE ID: CVE-2025-24117**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122073	O-APP-MACO-040225/208

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Preservation of Permissions	27-Jan-2025	5.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Sequoia 15.3. An app may be able to access protected user data. **CVE ID: CVE-2025-24087**	https://support.apple.com/en-us/122068	O-APP-MACO-040225/209
N/A	27-Jan-2025	5.5	This issue was addressed through improved state management. This issue is fixed in macOS Sequoia 15.3. A malicious app may be able to access arbitrary files. **CVE ID: CVE-2025-24096**	https://support.apple.com/en-us/122068	O-APP-MACO-040225/210
N/A	27-Jan-2025	5.3	This issue was addressed through improved state management. This issue is fixed in macOS Sequoia 15.3. Files downloaded from the internet may not have the quarantine flag applied. **CVE ID: CVE-2025-24140**	N/A	O-APP-MACO-040225/211
N/A	27-Jan-2025	4.3	The issue was addressed by adding additional logic. This issue is fixed in macOS Sequoia 15.3, Safari 18.3, iOS 18.3 and iPadOS 18.3. Visiting a malicious website may lead to address bar spoofing. **CVE ID: CVE-2025-24128**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122074	O-APP-MACO-040225/212
N/A	27-Jan-2025	4.3	The issue was addressed with improved UI. This issue is fixed in macOS Sequoia 15.3, Safari 18.3, iOS 18.3 and iPadOS 18.3, visionOS 2.3. Visiting a malicious website may lead to user interface spoofing. **CVE ID: CVE-2025-24113**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122073, https://support.apple.com/en-us/122074	O-APP-MACO-040225/213

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Information into Log File	27-Jan-2025	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sequoia 15.3, iOS 18.3 and iPadOS 18.3. An app may be able to view a contact's phone number in system logs. **CVE ID: CVE-2025-24145**	N/A	O-APP-MACO-040225/214
Affected Version(s): From (including) 14.0 Up to (excluding) 14.7.2					
N/A	27-Jan-2025	7.5	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Sonoma 14.7.2, macOS Sequoia 15.2, macOS Ventura 13.7.2. An attacker may gain access to protected parts of the file system. **CVE ID: CVE-2024-54557**	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	O-APP-MACO-040225/215
N/A	27-Jan-2025	5.5	This issue was addressed through improved state management. This issue is fixed in macOS Ventura 13.7.2, visionOS 2.2, tvOS 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sonoma 14.7.2, macOS Sequoia 15.2. An app may be able to access user-sensitive data. **CVE ID: CVE-2024-54541**	N/A	O-APP-MACO-040225/216
N/A	27-Jan-2025	5.3	A logic issue was addressed with improved file handling. This issue is fixed in macOS Ventura 13.7.2, iOS 18.2 and iPadOS 18.2, iPadOS 17.7.3, macOS Sonoma 14.7.2, macOS Sequoia 15.2. Photos in the Hidden Photos Album may be viewed without authentication. **CVE ID: CVE-2024-54488**	N/A	O-APP-MACO-040225/217
Affected Version(s): From (including) 14.0 Up to (excluding) 14.7.3					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	27-Jan-2025	7.8	An integer overflow was addressed through improved input validation. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. An app may be able to elevate privileges. **CVE ID: CVE-2025-24156**	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070	O-APP-MACO-040225/218
N/A	27-Jan-2025	7.5	This issue was addressed by improved management of object lifetimes. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. An attacker may be able to cause unexpected app termination. **CVE ID: CVE-2025-24120**	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070	O-APP-MACO-040225/219
N/A	27-Jan-2025	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, tvOS 18.3. Parsing a file may lead to an unexpected app termination. **CVE ID: CVE-2025-24127**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070, https://support.apple.com/en-us/122072	O-APP-MACO-040225/220
N/A	27-Jan-2025	5.5	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. An app may be able to modify protected parts of the file system.	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070	O-APP-MACO-040225/221

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-24114		
N/A	27-Jan-2025	5.5	The issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. Processing an image may lead to a denial-of-service. **CVE ID: CVE-2025-24086**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070, https://support.apple.com/en-us/122071	O-APP-MACO-040225/222
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	27-Jan-2025	4.7	A race condition was addressed with additional validation. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. An app may be able to access user-sensitive data. **CVE ID: CVE-2025-24094**	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070	O-APP-MACO-040225/223
Improper Link Resolution Before File Access ('Link Following')	27-Jan-2025	4.4	This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. A malicious app may be able to create symlinks to protected regions of the disk. **CVE ID: CVE-2025-24136**	N/A	O-APP-MACO-040225/224
N/A	27-Jan-2025	4.4	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. An app may be able to bypass Privacy preferences.	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070	O-APP-MACO-040225/225

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-24116		
N/A	27-Jan-2025	3.3	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. An app may be able to access information about a user's contacts. **CVE ID: CVE-2025-24100**	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070	O-APP-MACO-040225/226
N/A	27-Jan-2025	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.7.3, macOS Sonoma 14.7.3, macOS Sequoia 15. An app may be able to access contacts. **CVE ID: CVE-2024-44172**	N/A	O-APP-MACO-040225/227
Affected Version(s): From (including) 14.0 Up to (including) 14.7.3					
N/A	27-Jan-2025	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.2, tvOS 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sequoia 15.2. Processing web content may lead to a denial-of-service. **CVE ID: CVE-2024-54497**	N/A	O-APP-MACO-040225/228
Affected Version(s): From (including) 15.0 Up to (excluding) 15.2					
Out-of-bounds Write	27-Jan-2025	7.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Sonoma 14.7.2, macOS Sequoia 15.2, macOS Sonoma 14.7.3. An app may be able to cause unexpected system termination or write kernel memory.	N/A	O-APP-MACO-040225/229

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-54509		
N/A	27-Jan-2025	7.5	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Sonoma 14.7.2, macOS Sequoia 15.2, macOS Ventura 13.7.2. An attacker may gain access to protected parts of the file system. **CVE ID: CVE-2024-54557**	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	O-APP-MACO-040225/230
N/A	27-Jan-2025	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.2, tvOS 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sequoia 15.2. Processing web content may lead to a denial-of-service. **CVE ID: CVE-2024-54497**	N/A	O-APP-MACO-040225/231
N/A	27-Jan-2025	5.5	This issue was addressed through improved state management. This issue is fixed in macOS Ventura 13.7.2, visionOS 2.2, tvOS 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sonoma 14.7.2, macOS Sequoia 15.2. An app may be able to access user-sensitive data. **CVE ID: CVE-2024-54541**	N/A	O-APP-MACO-040225/232
N/A	27-Jan-2025	5.3	A logic issue was addressed with improved file handling. This issue is fixed in macOS Ventura 13.7.2, iOS 18.2 and iPadOS 18.2, iPadOS 17.7.3, macOS Sonoma 14.7.2, macOS Sequoia 15.2. Photos in the Hidden Photos Album may be viewed without authentication.	N/A	O-APP-MACO-040225/233

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-54488		
N/A	27-Jan-2025	3.3	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.7.2, macOS Sequoia 15.2. An app may be able to approve a launch daemon without user consent. **CVE ID: CVE-2024-54516**	N/A	O-APP-MACO-040225/234
Affected Version(s): From (including) 15.0 Up to (excluding) 15.3					
Integer Overflow or Wraparound	27-Jan-2025	7.8	An integer overflow was addressed through improved input validation. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. An app may be able to elevate privileges. **CVE ID: CVE-2025-24156**	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070	O-APP-MACO-040225/235
N/A	27-Jan-2025	7.5	This issue was addressed by improved management of object lifetimes. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. An attacker may be able to cause unexpected app termination. **CVE ID: CVE-2025-24120**	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070	O-APP-MACO-040225/236
NULL Pointer Dereference	27-Jan-2025	7.5	A null pointer dereference was addressed with improved input validation. This issue is fixed in macOS Sequoia 15.3, iOS 18.3 and iPadOS 18.3. A remote attacker may be able to cause a denial-of-service. **CVE ID: CVE-2025-24177**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068	O-APP-MACO-040225/237
N/A	27-Jan-2025	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Sonoma	https://support.apple.com/en-us/122066, https://support.	O-APP-MACO-040225/238

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. Parsing a file may lead to an unexpected app termination. **CVE ID: CVE-2025-24161**	apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072	
N/A	27-Jan-2025	5.5	The issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. Processing an image may lead to a denial-of-service. **CVE ID: CVE-2025-24086**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070, https://support.apple.com/en-us/122071	O-APP-MACO-040225/239
N/A	27-Jan-2025	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, tvOS 18.3. Parsing a file may lead to an unexpected app termination. **CVE ID: CVE-2025-24127**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070, https://support.apple.com/en-us/122072	O-APP-MACO-040225/240
N/A	27-Jan-2025	5.5	A permissions issue was addressed with additional	https://support.apple.com/en-	O-APP-MACO-040225/241

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restrictions. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. An app may be able to modify protected parts of the file system. **CVE ID: CVE-2025-24114**	us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070	
N/A	27-Jan-2025	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.3, macOS Sonoma 14.7.3. Parsing a file may lead to an unexpected app termination. **CVE ID: CVE-2025-24112**	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069	O-APP-MACO-040225/242
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	27-Jan-2025	4.7	A race condition was addressed with additional validation. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. An app may be able to access user-sensitive data. **CVE ID: CVE-2025-24094**	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070	O-APP-MACO-040225/243
Improper Link Resolution Before File Access ('Link Following')	27-Jan-2025	4.4	This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. A malicious app may be able to create symlinks to protected regions of the disk. **CVE ID: CVE-2025-24136**	N/A	O-APP-MACO-040225/244
N/A	27-Jan-2025	4.4	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. An app may be able to bypass Privacy preferences. **CVE ID: CVE-2025-24116**	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070	O-APP-MACO-040225/245

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	27-Jan-2025	3.3	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.3, macOS Sonoma 14.7.3. An app may be able to access information about a user's contacts. **CVE ID: CVE-2025-24100**	https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070	O-APP-MACO-040225/246
Product: tvos					
Affected Version(s): * Up to (excluding) 18.2					
Out-of-bounds Write	27-Jan-2025	8.8	The issue was addressed with improved memory handling. This issue is fixed in visionOS 2.2, tvOS 18.2, Safari 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sequoia 15.2. Processing maliciously crafted web content may lead to memory corruption. **CVE ID: CVE-2024-54543**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845, https://support.apple.com/en-us/121846	O-APP-TVOS-040225/247
Out-of-bounds Write	27-Jan-2025	7.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sequoia 15.2, watchOS 11.2, tvOS 18.2, iOS 18.2 and iPadOS 18.2. An app may be able to corrupt coprocessor memory. **CVE ID: CVE-2024-54522**	N/A	O-APP-TVOS-040225/248
Out-of-bounds Write	27-Jan-2025	7.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sequoia 15.2, watchOS 11.2, tvOS 18.2, iOS 18.2 and iPadOS 18.2. An app may be able to	N/A	O-APP-TVOS-040225/249

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			corrupt coprocessor memory. **CVE ID: CVE-2024-54517**		
N/A	27-Jan-2025	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.2, tvOS 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sequoia 15.2. Processing web content may lead to a denial-of-service. **CVE ID: CVE-2024-54497**	N/A	O-APP-TVOS-040225/250
N/A	27-Jan-2025	5.5	This issue was addressed through improved state management. This issue is fixed in macOS Ventura 13.7.2, visionOS 2.2, tvOS 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sonoma 14.7.2, macOS Sequoia 15.2. An app may be able to access user-sensitive data. **CVE ID: CVE-2024-54541**	N/A	O-APP-TVOS-040225/251
Affected Version(s): * Up to (excluding) 18.3					
Use After Free	27-Jan-2025	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. A malicious application may be able to elevate privileges. Apple is aware of a report that this issue may have been actively exploited against versions of iOS before iOS 17.2. **CVE ID: CVE-2025-24085**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072, https://support.apple.com/en-us/122073	O-APP-TVOS-040225/252
N/A	27-Jan-2025	7.8	A permissions issue was addressed with additional	https://support.apple.com/en-	O-APP-TVOS-040225/253

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restrictions. This issue is fixed in macOS Sequoia 15.3, tvOS 18.3, watchOS 11.3, iOS 18.3 and iPadOS 18.3. A malicious app may be able to gain root privileges. **CVE ID: CVE-2025-24107**	us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072	
Access of Resource Using Incompatible Type ('Type Confusion')	27-Jan-2025	7.5	A type confusion issue was addressed with improved checks. This issue is fixed in visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. A remote attacker may cause an unexpected app termination. **CVE ID: CVE-2025-24129**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072, https://support.apple.com/en-us/122073	O-APP-TVOS-040225/254
N/A	27-Jan-2025	6.5	The issue was addressed with improved memory handling. This issue is fixed in visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. An attacker in a privileged position may be able to perform a denial-of-service. **CVE ID: CVE-2025-24131**	N/A	O-APP-TVOS-040225/255
N/A	27-Jan-2025	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, tvOS 18.3. Parsing a file may lead to an unexpected app termination. **CVE ID: CVE-2025-24127**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-	O-APP-TVOS-040225/256

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/122070, https://support.apple.com/en-us/122072	
N/A	27-Jan-2025	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. Parsing a file may lead to an unexpected app termination. **CVE ID: CVE-2025-24161**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072	O-APP-TVOS-040225/257
N/A	27-Jan-2025	5.5	The issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. Processing an image may lead to a denial-of-service. **CVE ID: CVE-2025-24086**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070, https://support.apple.com/en-us/122071	O-APP-TVOS-040225/258
Product: visionos					
Affected Version(s): * Up to (excluding) 2.2					
Out-of-bounds Write	27-Jan-2025	8.8	The issue was addressed with improved memory handling. This issue is fixed in visionOS 2.2, tvOS 18.2, Safari 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sequoia 15.2. Processing maliciously	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-	O-APP-VISI-040225/259

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted web content may lead to memory corruption. **CVE ID: CVE-2024-54543**	us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845, https://support.apple.com/en-us/121846	
N/A	27-Jan-2025	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.2, tvOS 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sequoia 15.2. Processing web content may lead to a denial-of-service. **CVE ID: CVE-2024-54497**	N/A	O-APP-VISI-040225/260
N/A	27-Jan-2025	5.5	This issue was addressed through improved state management. This issue is fixed in macOS Ventura 13.7.2, visionOS 2.2, tvOS 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sonoma 14.7.2, macOS Sequoia 15.2. An app may be able to access user-sensitive data. **CVE ID: CVE-2024-54541**	N/A	O-APP-VISI-040225/261
Affected Version(s): * Up to (excluding) 2.3					
Use After Free	27-Jan-2025	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. A malicious application may be able to elevate privileges. Apple is aware of a report that this issue may have been actively	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072, https://support.	O-APP-VISI-040225/262

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploited against versions of iOS before iOS 17.2. **CVE ID: CVE-2025-24085**	apple.com/en-us/122073	
Access of Resource Using Incompatible Type ('Type Confusion')	27-Jan-2025	7.5	A type confusion issue was addressed with improved checks. This issue is fixed in visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. A remote attacker may cause an unexpected app termination. **CVE ID: CVE-2025-24129**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072, https://support.apple.com/en-us/122073	O-APP-VISI-040225/263
N/A	27-Jan-2025	6.5	The issue was addressed with improved memory handling. This issue is fixed in visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. An attacker in a privileged position may be able to perform a denial-of-service. **CVE ID: CVE-2025-24131**	N/A	O-APP-VISI-040225/264
N/A	27-Jan-2025	6.5	The issue was addressed with improved access restrictions to the file system. This issue is fixed in macOS Sequoia 15.3, Safari 18.3, iOS 18.3 and iPadOS 18.3, visionOS 2.3. A maliciously crafted webpage may be able to fingerprint the user. **CVE ID: CVE-2025-24143**	N/A	O-APP-VISI-040225/265
N/A	27-Jan-2025	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, tvOS	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-	O-APP-VISI-040225/266

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			18.3. Parsing a file may lead to an unexpected app termination. **CVE ID: CVE-2025-24127**	us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070, https://support.apple.com/en-us/122072	
Insecure Storage of Sensitive Information	27-Jan-2025	5.5	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iPadOS 17.7.4, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3. An app may be able to fingerprint the user. **CVE ID: CVE-2025-24117**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122073	O-APP-VISI-040225/267
N/A	27-Jan-2025	5.5	The issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. Processing an image may lead to a denial-of-service. **CVE ID: CVE-2025-24086**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122070, https://support.apple.com/en-us/122071	O-APP-VISI-040225/268
N/A	27-Jan-2025	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. Parsing a file may lead to an	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068,	O-APP-VISI-040225/269

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected app termination. **CVE ID: CVE-2025-24161**	https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072	
N/A	27-Jan-2025	4.3	The issue was addressed with improved UI. This issue is fixed in macOS Sequoia 15.3, Safari 18.3, iOS 18.3 and iPadOS 18.3, visionOS 2.3. Visiting a malicious website may lead to user interface spoofing. **CVE ID: CVE-2025-24113**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122073, https://support.apple.com/en-us/122074	O-APP-VISI-040225/270
Product: watchos					
Affected Version(s): * Up to (excluding) 11.2					
N/A	27-Jan-2025	9.1	The issue was addressed by removing the relevant flags. This issue is fixed in watchOS 11.2, iOS 18.2 and iPadOS 18.2. A system binary could be used to fingerprint a user's Apple Account. **CVE ID: CVE-2024-54512**	N/A	O-APP-WATC-040225/271
Out-of-bounds Write	27-Jan-2025	8.8	The issue was addressed with improved memory handling. This issue is fixed in visionOS 2.2, tvOS 18.2, Safari 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sequoia 15.2. Processing maliciously crafted web content may lead to memory corruption. **CVE ID: CVE-2024-54543**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845, https://support.	O-APP-WATC-040225/272

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				apple.com/en-us/121846	
Out-of-bounds Write	27-Jan-2025	7.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sequoia 15.2, watchOS 11.2, tvOS 18.2, iOS 18.2 and iPadOS 18.2. An app may be able to corrupt coprocessor memory. **CVE ID: CVE-2024-54522**	N/A	O-APP-WATC-040225/273
Out-of-bounds Write	27-Jan-2025	7.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sequoia 15.2, watchOS 11.2, tvOS 18.2, iOS 18.2 and iPadOS 18.2. An app may be able to corrupt coprocessor memory. **CVE ID: CVE-2024-54517**	N/A	O-APP-WATC-040225/274
N/A	27-Jan-2025	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.2, tvOS 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sequoia 15.2. Processing web content may lead to a denial-of-service. **CVE ID: CVE-2024-54497**	N/A	O-APP-WATC-040225/275
N/A	27-Jan-2025	5.5	This issue was addressed through improved state management. This issue is fixed in macOS Ventura 13.7.2, visionOS 2.2, tvOS 18.2, watchOS 11.2, iOS 18.2 and iPadOS 18.2, macOS Sonoma 14.7.2, macOS Sequoia 15.2. An app may be able to access user-sensitive data. **CVE ID: CVE-2024-54541**	N/A	O-APP-WATC-040225/276

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 11.3					
Use After Free	27-Jan-2025	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. A malicious application may be able to elevate privileges. Apple is aware of a report that this issue may have been actively exploited against versions of iOS before iOS 17.2. **CVE ID: CVE-2025-24085**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072, https://support.apple.com/en-us/122073	O-APP-WATC-040225/277
N/A	27-Jan-2025	7.8	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.3, tvOS 18.3, watchOS 11.3, iOS 18.3 and iPadOS 18.3. A malicious app may be able to gain root privileges. **CVE ID: CVE-2025-24107**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072	O-APP-WATC-040225/278
Access of Resource Using Incompatible Type ('Type Confusion')	27-Jan-2025	7.5	A type confusion issue was addressed with improved checks. This issue is fixed in visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. A remote attacker may cause an unexpected app termination. **CVE ID: CVE-2025-24129**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072, https://support.apple.com/en-us/122073	O-APP-WATC-040225/279
N/A	27-Jan-2025	6.5	The issue was addressed with improved memory handling. This issue is fixed in visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. An attacker in a	N/A	O-APP-WATC-040225/280

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged position may be able to perform a denial-of-service. **CVE ID: CVE-2025-24131**		
Insecure Storage of Sensitive Information	27-Jan-2025	5.5	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iPadOS 17.7.4, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3. An app may be able to fingerprint the user. **CVE ID: CVE-2025-24117**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122073	O-APP-WATC-040225/281
N/A	27-Jan-2025	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.4, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. Parsing a file may lead to an unexpected app termination. **CVE ID: CVE-2025-24161**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.apple.com/en-us/122071, https://support.apple.com/en-us/122072	O-APP-WATC-040225/282
N/A	27-Jan-2025	5.5	The issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.4, macOS Ventura 13.7.3, macOS Sonoma 14.7.3, visionOS 2.3, iOS 18.3 and iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, tvOS 18.3. Processing an image may lead to a denial-of-service. **CVE ID: CVE-2025-24086**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122067, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122069, https://support.	O-APP-WATC-040225/283

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				apple.com/en-us/122070, https://support.apple.com/en-us/122071	
Vendor: Google					
Product: android					
Affected Version(s): -					
Out-of-bounds Write	18-Jan-2025	7.8	In ip6_append_data of ip6_output.c, there is a possible way to achieve code execution due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID: CVE-2018-9389**	https://source.android.com/security/bulletin/pixel/2018-06-01	O-GOO-ANDR-040225/284
Missing Authorization	18-Jan-2025	5.5	In NlpService, there is a possible way to obtain location information due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID: CVE-2018-9406**	https://source.android.com/security/bulletin/pixel/2018-06-01	O-GOO-ANDR-040225/285
Affected Version(s): 6.0					
N/A	17-Jan-2025	5.5	In endCallForSubscriber of PhoneInterfaceManager.java, there is a possible way to prevent access to emergency services due to a logic error in the code. This could lead to a local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID: CVE-2017-13322**	https://source.android.com/security/bulletin/pixel/2018-05-01	O-GOO-ANDR-040225/286

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 6.0.1					
N/A	17-Jan-2025	5.5	In endCallForSubscriber of PhoneInterfaceManager.java, there is a possible way to prevent access to emergency services due to a logic error in the code. This could lead to a local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID: CVE-2017-13322**	https://source.android.com/security/bulletin/pixel/2018-05-01	O-GOO-ANDR-040225/287
Affected Version(s): 7.0					
N/A	17-Jan-2025	5.5	In endCallForSubscriber of PhoneInterfaceManager.java, there is a possible way to prevent access to emergency services due to a logic error in the code. This could lead to a local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID: CVE-2017-13322**	https://source.android.com/security/bulletin/pixel/2018-05-01	O-GOO-ANDR-040225/288
Affected Version(s): 7.1.1					
N/A	17-Jan-2025	5.5	In endCallForSubscriber of PhoneInterfaceManager.java, there is a possible way to prevent access to emergency services due to a logic error in the code. This could lead to a local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID: CVE-2017-13322**	https://source.android.com/security/bulletin/pixel/2018-05-01	O-GOO-ANDR-040225/289
Affected Version(s): 7.1.2					
N/A	17-Jan-2025	5.5	In endCallForSubscriber of PhoneInterfaceManager.java, there is a possible way to	https://source.android.com/sec	O-GOO-ANDR-040225/290

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prevent access to emergency services due to a logic error in the code. This could lead to a local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID: CVE-2017-13322**	urity/bulletin/pixel/2018-05-01	
Affected Version(s): 8.0					
N/A	17-Jan-2025	5.5	In endCallForSubscriber of PhoneInterfaceManager.java, there is a possible way to prevent access to emergency services due to a logic error in the code. This could lead to a local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID: CVE-2017-13322**	https://source.android.com/security/bulletin/pixel/2018-05-01	O-GOO-ANDR-040225/291
Affected Version(s): 8.1					
N/A	17-Jan-2025	5.5	In endCallForSubscriber of PhoneInterfaceManager.java, there is a possible way to prevent access to emergency services due to a logic error in the code. This could lead to a local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID: CVE-2017-13322**	https://source.android.com/security/bulletin/pixel/2018-05-01	O-GOO-ANDR-040225/292
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): 6.13					
Use After Free	19-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/078b2ff7da200b7532398e668ee	O-LIN-LINU-040225/293

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drm/mediatek: Set private->all_drm_private[i]->drm to NULL if mtk_drm_bind returns err The pointer need to be set to NULL, otherwise KASAN complains about use-after-free. Because in mtk_drm_bind, all private's drm are set as follows. private->all_drm_private[i]->drm = drm; And drm will be released by drm_dev_put in case mtk_drm_kms_init returns failure. However, the shutdown path still accesses the previous allocated memory in drm_atomic_helper_shutdown. [84.874820] watchdog: watchdog0: watchdog did not stop! [86.512054] ========== [86.513162] BUG: KASAN: use-after-free in drm_atomic_helper_shutdown+0x33c/0x378 [86.514258] Read of size 8 at addr ffff0000d46fc068 by task shutdown/1 [86.515213] [86.515455] CPU: 1 UID: 0 PID: 1 Comm: shutdown Not tainted 6.13.0-rc1-mtk+gfa1a78e5d24b-dirty #55 [86.516752] Hardware name: Unknown Product/Unknown	f723ad40fb516, https://git.kernel.org/stable/c/36684e9d88a2e2401ae26715a2e217cb4295cea7, https://git.kernel.org/stable/c/7083b93e9755d60f0c2bcaa9d064308108280534	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Product, BIOS 2022.10 10/01/2022 [86.517960] Call trace: [86.518333] show_stack+0x20/0x38 (C) [86.518891] dump_stack_lvl+0x90/0xd 0 [86.519443] print_report+0xf8/0x5b0 [86.519985] kasan_report+0xb4/0x100 [86.520526] __asan_report_load8_noabo rt+0x20/0x30 [86.521240] drm_atomic_helper_shutdo wn+0x33c/0x378 [86.521966] mtk_drm_shutdown+0x54/ 0x80 [86.522546] platform_shutdown+0x64/ 0x90 [86.523137] device_shutdown+0x260/0 x5b8 [86.523728] kernel_restart+0x78/0xf0 [86.524282] __do_sys_reboot+0x258/0x 2f0 [86.524871] __arm64_sys_reboot+0x90/ 0xd8 [86.525473] invoke_syscall+0x74/0x26 8 [86.526041] el0_svc_common.constprop .0+0xb0/0x240 [86.526751] do_el0_svc+0x4c/0x70 [86.527251] el0_svc+0x4c/0xc0 [86.527719] el0t_64_sync_handler+0x1 44/0x168 [86.528367] el0t_64_sync+0x198/0x1a 0 [86.528920]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[86.529157] The buggy address belongs to the physical page: [86.529972] page: refcount:0 mapcount:0 mapping:0000000000000000 index:0xffff0000d46fd4d0 pfn:0x1146fc [86.531319] flags: 0xbfffc0000000000(node=0|zone=2|lastcpupid=0xffff) [86.532267] raw: 0bfffc0000000000 0000000000000000 dead000000000122 0000000000000000 [86.533390] raw: ffff0000d46fd4d0 0000000000000000 00000000ffffffff 0000000000000000 [86.534511] page dumped because: kasan: bad access detected [86.535323] [86.535559] Memory state around the buggy address: [86.536265] ffff0000d46fbf00: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff [86.537314] ffff0000d46fbf80: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff [86.538363] >ffff0000d46fc000: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff [86.544733] ^ [86.551057] ffff0000d46fc080: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff [86.557510] ffff0000d46fc100: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff [86.563928] ========== ==========		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[86.571093] Disabling lock debugging due to kernel taint [86.577642] Unable to handle kernel paging request at virtual address e0e9c0920000000b [86.581834] KASAN: maybe wild-memory-access in range [0x0752049000000058-0x075204900000005f] ... **CVE ID: CVE-2024-57926**		
NULL Pointer Dereference	19-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: nfs: Fix oops in nfs_netfs_init_request() when copying to cache When netfslib wants to copy some data that has just been read on behalf of nfs, it creates a new write request and calls nfs_netfs_init_request() to initialise it, but with a NULL file pointer. This causes nfs_file_open_context() to oops - however, we don't actually need the nfs context as we're only going to write to the cache. Fix this by just returning if we aren't given a file pointer and emit a warning if the request was for something other than copy-to-cache. Further, fix nfs_netfs_free_request() so that it doesn't try to free the context if the pointer is NULL. **CVE ID: CVE-2024-57927**	https://git.kernel.org/stable/c/13a07cc81e2d116cece727a83746c74b87a9d417, https://git.kernel.org/stable/c/86ad1a58f6a9453f49e06ef957a40a8dac00a13f	O-LIN-LINU-040225/294

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	21-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: gve: guard XSK operations on the existence of queues This patch predicates the enabling and disabling of XSK pools on the existence of queues. As it stands, if the interface is down, disabling or enabling XSK pools would result in a crash, as the RX queue pointer would be NULL. XSK pool registration will occur as part of the next interface up. Similarly, xsk_wakeup needs be guarded against queues disappearing while the function is executing, so a check against the GVE_PRIV_FLAGS_NAPI_ENABLED flag is added to synchronize with the disabling of the bit and the synchronize_net() in gve_turndown. **CVE ID: CVE-2024-57933**	https://git.kernel.org/stable/c/40338d7987d810fcaa95c500b1068a52b08eec9b, https://git.kernel.org/stable/c/771d66f2bd8c4dba1286a9163ab982cecd825718, https://git.kernel.org/stable/c/8e8d7037c89437af12725f454e2eaf40e8166c0f	O-LIN-LINU-040225/295
NULL Pointer Dereference	19-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Fix tlb invalidation when wedging If GuC fails to load, the driver wedges, but in the process it tries to do stuff that may not be initialized yet. This moves the xe_gt_tlb_invalidation_init() to be done earlier: as its own doc says,	https://git.kernel.org/stable/c/09b94ddc58c6640cbbc7775a61a5387b8be71488, https://git.kernel.org/stable/c/9ab4981552930a9c45682d62424ba610edc3992d	O-LIN-LINU-040225/296

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			it's a software-only initialization and should had been named with the _early() suffix. Move it to be called by xe_gt_init_early(), so the locks and seqno are initialized, avoiding a NULL ptr deref when wedging: xe 0000:03:00.0: [drm] *ERROR* GT0: load failed: status: Reset = 0, BootROM = 0x50, UKernel = 0x00, MIA = 0x00, Auth = 0x01 xe 0000:03:00.0: [drm] *ERROR* GT0: firmware signature verification failed xe 0000:03:00.0: [drm] *ERROR* CRITICAL: Xe has declared device 0000:03:00.0 as wedged. ... BUG: kernel NULL pointer dereference, address: 0000000000000000 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 9 UID: 0 PID: 3908 Comm: modprobe Tainted: G U W 6.13.0-rc4-xe+ #3 Tainted: [U]=USER, [W]=WARN Hardware name: Intel Corporation Alder Lake Client Platform/AlderLake-S ADP-S DDR5 UDIMM CRB, BIOS ADLSFWI1.R00.3275.A00.2207010640 07/01/2022		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RIP: 0010:xe_gt_tlb_invalidation_reset+0x75/0x110 [xe] This can be easily triggered by poking the GuC binary to force a signature failure. There will still be an extra message, xe 0000:03:00.0: [drm] *ERROR* GT0: GuC mmio request 0x4100: no reply 0x4100 but that's better than a NULL ptr deref. (cherry picked from commit 5001ef3af8f2c972d6fd9c5221a8457556f8bea6) **CVE ID: CVE-2025-21644**		
NULL Pointer Dereference	19-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net: hns3: fix kernel crash when 1588 is sent on HIP08 devices Currently, HIP08 devices does not register the ptp devices, so the hdev->ptp is NULL. But the tx process would still try to set hardware time stamp info with SKBTX_HW_TSTAMP flag and cause a kernel crash. [128.087798] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000018 ... [128.280251] pc : hclge_ptp_set_tx_info+0x2c/0x140 [hclge]	https://git.kernel.org/stable/c/9741e72b2286de8b38de9db685588ac421a95c87, https://git.kernel.org/stable/c/f19ab3ef96d9626e5f1bdc56d3574c355e83d623	O-LIN-LINU-040225/297

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[128.286600] lr : hclge_ptp_set_tx_info+0x20 /0x140 [hclge] [128.292938] sp : ffff800059b93140 [128.297200] x29: ffff800059b93140 x28: 0000000000003280 [128.303455] x27: ffff800020d48280 x26: ffff0cb9dc814080 [128.309715] x25: ffff0cb9cde93fa0 x24: 0000000000000001 [128.315969] x23: 0000000000000000 x22: 0000000000000194 [128.322219] x21: ffff0cd94f986000 x20: 0000000000000000 [128.328462] x19: ffff0cb9d2a166c0 x18: 0000000000000000 [128.334698] x17: 0000000000000000 x16: ffffcf1fc523ed24 [128.340934] x15: 0000ffffd530a518 x14: 0000000000000000 [128.347162] x13: ffff0cd6bdb31310 x12: 0000000000000368 [128.353388] x11: ffff0cb9cfbc7070 x10: ffff2cf55dd11e02 [128.359606] x9 : ffffcf1f85a212b4 x8 : ffff0cd7cf27dab0 [128.365831] x7 : 0000000000000a20 x6 : ffff0cd7cf27d000 [128.372040] x5 : 0000000000000000 x4 : 000000000000ffff [128.378243] x3 : 0000000000000400 x2 : ffffcf1f85a21294 [128.384437] x1 : ffff0cb9db520080 x0 : ffff0cb9db500080 [128.390626] Call trace: [128.393964]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hclge_ptp_set_tx_info+0x2c /0x140 [hclge] [128.399893] hns3_nic_net_xmit+0x39c/ 0x4c4 [hns3] [128.405468] xmit_one.constprop.0+0xc 4/0x200 [128.410600] dev_hard_start_xmit+0x54 /0xf0 [128.415556] sch_direct_xmit+0xe8/0x6 34 [128.420246] __dev_queue_xmit+0x224/ 0xc70 [128.425101] dev_queue_xmit+0x1c/0x4 0 [128.429608] ovs_vport_send+0xac/0x1a 0 [openvswitch] [128.435409] do_output+0x60/0x17c [openvswitch] [128.440770] do_execute_actions+0x898 /0x8c4 [openvswitch] [128.446993] ovs_execute_actions+0x64/ 0xf0 [openvswitch] [128.453129] ovs_dp_process_packet+0x a0/0x224 [openvswitch] [128.459530] ovs_vport_receive+0x7c/0x fc [openvswitch] [128.465497] internal_dev_xmit+0x34/0 xb0 [openvswitch] [128.471460] xmit_one.constprop.0+0xc 4/0x200 [128.476561] dev_hard_start_xmit+0x54 /0xf0 [128.481489] __dev_queue_xmit+0x968/ 0xc70 [128.486330] dev_queue_xmit+0x1c/0x4		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0 [128.490856] ip_finish_output2+0x250/0x570 [128.495810] __ip_finish_output+0x170/0x1e0 [128.500832] ip_finish_output+0x3c/0xf0 [128.505504] ip_output+0xbc/0x160 [128.509654] ip_send_skb+0x58/0xd4 [128.513892] udp_send_skb+0x12c/0x354 [128.518387] udp_sendmsg+0x7a8/0x9c0 [128.522793] inet_sendmsg+0x4c/0x8c [128.527116] __sock_sendmsg+0x48/0x80 [128.531609] __sys_sendto+0x124/0x164 [128.536099] __arm64_sys_sendto+0x30/0x5c [128.540935] invoke_syscall+0x50/0x130 [128.545508] el0_svc_common.constprop.0+0x10c/0x124 [128.551205] do_el0_svc+0x34/0xdc [128.555347] el0_svc+0x20/0x30 [128.559227] el0_sync_handler+0xb8/0xc0 [128.563883] el0_sync+0x160/0x180 **CVE ID: CVE-2025-21649**		
Integer Overflow or Wraparound	21-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/081bdb3a31674	O-LIN-LINU-040225/298

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/sctp: Prevent autoclose integer overflow in sctp_association_init() While by default max_autoclose equals to INT_MAX / HZ, one may set net.sctp.max_autoclose to UINT_MAX. There is code in sctp_association_init() that can consequently trigger overflow. **CVE ID: CVE-2024-57938**	339313c6d702af922bc29de2c53, https://git.kernel.org/stable/c/2297890b778b0e7c8200d6818154f7e461d78e94, https://git.kernel.org/stable/c/271f031f4c31c07e2a85a1ba2b4c8e734909a477	
Loop with Unreachable Exit Condition ('Infinite Loop')	21-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: exfat: fix the infinite loop in exfat_readdir() If the file system is corrupted so that a cluster is linked to itself in the cluster chain, and there is an unused directory entry in the cluster, 'dentry' will not be incremented, causing condition 'dentry < max_dentries' unable to prevent an infinite loop. This infinite loop causes s_lock not to be released, and other tasks will hang, such as exfat_sync_fs(). This commit stops traversing the cluster chain when there is unused directory entry in the cluster to avoid this infinite loop. **CVE ID: CVE-2024-57940**	https://git.kernel.org/stable/c/31beabd0f47f8c3ed9965ba861c9e5b252d4920a, https://git.kernel.org/stable/c/d9ea94f5cd117d56e573696d0045ab3044185a15, https://git.kernel.org/stable/c/dc1d7afceb982e8f666e70a582e6b5aa806de063	O-LIN-LINU-040225/299
NULL Pointer Dereference	19-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/8586d6ea623e4	O-LIN-LINU-040225/300

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			usb: typec: tcpci: fix NULL pointer issue on shared irq case The tcpci_irq() may meet below NULL pointer dereference issue: [2.641851] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000010 [2.641951] status 0x1, 0x37f [2.650659] Mem abort info: [2.656490] ESR = 0x0000000096000004 [2.660230] EC = 0x25: DABT (current EL), IL = 32 bits [2.665532] SET = 0, FnV = 0 [2.668579] EA = 0, S1PTW = 0 [2.671715] FSC = 0x04: level 0 translation fault [2.676584] Data abort info: [2.679459] ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 [2.684936] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [2.689980] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [2.695284] [0000000000000010] user address but active_mm is swapper [2.701632] Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP [2.707883] Modules linked in: [2.710936] CPU: 1 UID: 0 PID: 87 Comm: irq/111-2-0051 Not tainted 6.12.0-rc6-06316-g7f63786ad3d1-dirty #4	8b2bd38304bbc52b0b8228816ff, https://git.kernel.org/stable/c/862a9c0f68487fd6ced15622d9cdcec48f8b5aaa	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[2.720570] Hardware name: NXP i.MX93 11X11 EVK board (DT) [2.726040] pstate: 60400009 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) [2.732989] pc : tcpci_irq+0x38/0x318 [2.736647] lr : _tcpci_irq+0x14/0x20 [2.740295] sp : ffff80008324bd30 [2.743597] x29: ffff80008324bd70 x28: ffff800080107894 x27: ffff800082198f70 [2.750721] x26: ffff0000050e6680 x25: ffff000004d172ac x24: ffff0000050f0000 [2.757845] x23: ffff000004d17200 x22: 0000000000000001 x21: ffff0000050f0000 [2.764969] x20: ffff000004d17200 x19: 0000000000000000 x18: 0000000000000001 [2.772093] x17: 0000000000000000 x16: ffff80008183d8a0 x15: ffff00007fbab040 [2.779217] x14: ffff00007fb918c0 x13: 0000000000000000 x12: 000000000000017a [2.786341] x11: 0000000000000001 x10: 0000000000000a90 x9 : ffff80008324bd00 [2.793465] x8 : ffff0000050f0af0 x7 : ffff00007fbaa840 x6 : 0000000000000031 [2.800589] x5 : 000000000000017a x4 : 0000000000000002 x3 : 0000000000000002 [2.807713] x2 : ffff80008324bd3a x1 : 0000000000000010 x0 :		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000000 [2.814838] Call trace: [2.817273] tcpci_irq+0x38/0x318 [2.820583] _tcpci_irq+0x14/0x20 [2.823885] irq_thread_fn+0x2c/0xa8 [2.827456] irq_thread+0x16c/0x2f4 [2.830940] kthread+0x110/0x114 [2.834164] ret_from_fork+0x10/0x20 [2.837738] Code: f9426420 f9001fe0 d2800000 52800201 (f9400a60) This may happen on shared irq case. Such as two Type-C ports share one irq. After the first port finished tcpci_register_port(), it may trigger interrupt. However, if the interrupt comes by chance the 2nd port finishes devm_request_threaded_irq(), the 2nd port interrupt handler will run at first. Then the above issue happens due to tcpci is still a NULL pointer in tcpci_irq() when dereference to regmap. devm_request_threaded_irq() <-- port1 irq comes disable_irq(client->irq); tcpci_register_port() This will restore the logic to the state before commit (77e85107a771 "usb: typec: tcpci: support edge irq").		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			However, moving tcpci_register_port() earlier creates a problem when use edge irq because tcpci_init() will be called before devm_request_threaded_irq(). The tcpci_init() writes the ALERT_MASK to the hardware to tell it to start generating interrupts but we're not ready to deal with them yet, then the ALERT events may be missed and ALERT line will not recover to high level forever. To avoid the issue, this will also set ALERT_MASK register after devm_request_threaded_irq() return. **CVE ID: CVE-2024-57914**		
NULL Pointer Dereference	21-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: iio: adc: ti-ads1298: Add NULL check in ads1298_init devm_kasprintf() can return a NULL pointer on failure. A check on the return value of such a call in ads1298_init() is missing. Add it. **CVE ID: CVE-2024-57944**	https://git.kernel.org/stable/c/69b680bbac9bd611aaa308769d6c71e3e70eb3c3, https://git.kernel.org/stable/c/bcb394bb28e55312cace75362b8e489eb0e02a30	O-LIN-LINU-040225/301
NULL Pointer Dereference	21-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: avoid NULL pointer dereference if no valid extent tree [BUG] Syzbot reported a crash with the following call trace:	https://git.kernel.org/stable/c/24b85a8b0310e0144da9ab30be42e87e6476638a, https://git.kernel.org/stable/c/6aecd91a5c5b68939cf4169e32bc49f3cd2dd329,	O-LIN-LINU-040225/302

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BTRFS info (device loop0): scrub: started on devid 1 BUG: kernel NULL pointer dereference, address: 0000000000000208 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 106e70067 P4D 106e70067 PUD 107143067 PMD 0 Oops: Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 1 UID: 0 PID: 689 Comm: repro Kdump: loaded Tainted: G O 6.13.0-rc4-custom+ #206 Tainted: [O]=OOT_MODULE Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS unknown 02/02/2022 RIP: 0010:find_first_extent_item +0x26/0x1f0 [btrfs] Call Trace: <TASK> scrub_find_fill_first_stripe+ 0x13d/0x3b0 [btrfs] scrub_simple_mirror+0x17 5/0x260 [btrfs] scrub_stripe+0x5d4/0x6c0 [btrfs] scrub_chunk+0xbb/0x170 [btrfs] scrub_enumerate_chunks+ 0x2f4/0x5f0 [btrfs] btrfs_scrub_dev+0x240/0x 600 [btrfs] btrfs_ioctl+0x1dc8/0x2fa0 [btrfs] ?	https://git.kernel.org/stable/c/aee5f69f3e6cd82bfefaca1b70b40b6cd8f3f784	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_sys_openat2+0xa5/0xf0 __x64_sys_ioctl+0x97/0xc0 do_syscall_64+0x4f/0x120 entry_SYSCALL_64_after_hwframe+0x76/0x7e </TASK> [CAUSE] The reproducer is using a corrupted image where extent tree root is corrupted, thus forcing to use "rescue=all,ro" mount option to mount the image. Then it triggered a scrub, but since scrub relies on extent tree to find where the data/metadata extents are, scrub_find_fill_first_stripe() relies on an non-empty extent root. But unfortunately scrub_find_fill_first_stripe() doesn't really expect an NULL pointer for extent root, it use extent_root to grab fs_info and triggered a NULL pointer dereference. [FIX] Add an extra check for a valid extent root at the beginning of scrub_find_fill_first_stripe(). The new error path is introduced by 42437a6386ff ("btrfs: introduce mount option rescue=ignorebadroots"), but that's pretty old, and later		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commit b979547513ff ("btrfs: scrub: introduce helper to find and fill sector info for a scrub_stripe") changed how we do scrub. So for kernels older than 6.6, the fix will need manual backport. **CVE ID: CVE-2025-21658**		
NULL Pointer Dereference	19-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: u_serial: Disable ep before setting port to null to fix the crash caused by port being null Considering that in some extreme cases, when performing the unbinding operation, gserial_disconnect has cleared gser->ioport, which triggers gadget reconfiguration, and then calls gs_read_complete, resulting in access to a null pointer. Therefore, ep is disabled before gserial_disconnect sets port to null to prevent this from happening. Call trace: gs_read_complete+0x58/0x240 usb_gadget_giveback_request+0x40/0x160 dwc3_remove_requests+0x170/0x484 dwc3_ep0_out_start+0xb0/0x1d4	https://git.kernel.org/stable/c/0c50f00cc29948184af05bda31392fff5821f4f3, https://git.kernel.org/stable/c/13014969cbf07f18d62ceea40bd8ca8ec9d36cec, https://git.kernel.org/stable/c/3d730e8758c75b68a0152ee1ac48a270ea6725b4	O-LIN-LINU-040225/303

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__dwc3_gadget_start+0x25c/0x720 kretprobe_trampoline.cfi_jt+0x0/0x8 kretprobe_trampoline.cfi_jt+0x0/0x8 udc_bind_to_driver+0x1d8/0x300 usb_gadget_probe_driver+0xa8/0x1dc gadget_dev_desc_UDC_store+0x13c/0x188 configfs_write_iter+0x160/0x1f4 vfs_write+0x2d0/0x40c ksys_write+0x7c/0xf0 __arm64_sys_write+0x20/0x30 invoke_syscall+0x60/0x150 el0_svc_common+0x8c/0xf8 do_el0_svc+0x28/0xa0 el0_svc+0x24/0x84 **CVE ID: CVE-2024-57915**		
Affected Version(s): From (including) 2.6.27 Up to (excluding) 6.1.125					
NULL Pointer Dereference	19-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: u_serial: Disable ep before setting port to null to fix the crash caused by port being null Considering that in some extreme cases, when performing the unbinding operation, gserial_disconnect has cleared gser->ioport,	https://git.kernel.org/stable/c/0c50f00cc29948184af05bda31392fff5821f4f3, https://git.kernel.org/stable/c/13014969cbf07f18d62ceea40bd8ca8ec9d36cec, https://git.kernel.org/stable/c/3d730e8758c75b68a0152ee1ac	O-LIN-LINU-040225/304

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which triggers gadget reconfiguration, and then calls gs_read_complete, resulting in access to a null pointer. Therefore, ep is disabled before gserial_disconnect sets port to null to prevent this from happening. Call trace: gs_read_complete+0x58/0x240 usb_gadget_giveback_request+0x40/0x160 dwc3_remove_requests+0x170/0x484 dwc3_ep0_out_start+0xb0/0x1d4 __dwc3_gadget_start+0x25c/0x720 kretprobe_trampoline.cfi_jt+0x0/0x8 kretprobe_trampoline.cfi_jt+0x0/0x8 udc_bind_to_driver+0x1d8/0x300 usb_gadget_probe_driver+0xa8/0x1dc gadget_dev_desc_UDC_store+0x13c/0x188 configfs_write_iter+0x160/0x1f4 vfs_write+0x2d0/0x40c ksys_write+0x7c/0xf0 __arm64_sys_write+0x20/0x30 invoke_syscall+0x60/0x150	48a270ea6725b4	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			el0_svc_common+0x8c/0xf8 do_el0_svc+0x28/0xa0 el0_svc+0x24/0x84 **CVE ID: CVE-2024-57915**		
Affected Version(s): From (including) 3.13 Up to (excluding) 5.4.289					
Integer Overflow or Wraparound	21-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net/sctp: Prevent autoclose integer overflow in sctp_association_init() While by default max_autoclose equals to INT_MAX / HZ, one may set net.sctp.max_autoclose to UINT_MAX. There is code in sctp_association_init() that can consequently trigger overflow. **CVE ID: CVE-2024-57938**	https://git.kernel.org/stable/c/081bdb3a31674339313c6d702af922bc29de2c53, https://git.kernel.org/stable/c/2297890b778b0e7c8200d6818154f7e461d78e94, https://git.kernel.org/stable/c/271f031f4c31c07e2a85a1ba2b4c8e734909a477	O-LIN-LINU-040225/305
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.176					
Integer Overflow or Wraparound	21-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net/sctp: Prevent autoclose integer overflow in sctp_association_init() While by default max_autoclose equals to INT_MAX / HZ, one may set net.sctp.max_autoclose to UINT_MAX. There is code in sctp_association_init() that can consequently trigger overflow. **CVE ID: CVE-2024-57938**	https://git.kernel.org/stable/c/081bdb3a31674339313c6d702af922bc29de2c53, https://git.kernel.org/stable/c/2297890b778b0e7c8200d6818154f7e461d78e94, https://git.kernel.org/stable/c/271f031f4c31c07e2a85a1ba2b4c8e734909a477	O-LIN-LINU-040225/306
Affected Version(s): From (including) 5.11 Up to (excluding) 6.6.72					
NULL Pointer Dereference	21-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/24b85a8b0310e	O-LIN-LINU-040225/307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			btrfs: avoid NULL pointer dereference if no valid extent tree [BUG] Syzbot reported a crash with the following call trace: BTRFS info (device loop0): scrub: started on devid 1 BUG: kernel NULL pointer dereference, address: 0000000000000208 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 106e70067 P4D 106e70067 PUD 107143067 PMD 0 Oops: Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 1 UID: 0 PID: 689 Comm: repro Kdump: loaded Tainted: G O 6.13.0-rc4-custom+ #206 Tainted: [O]=OOT_MODULE Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS unknown 02/02/2022 RIP: 0010:find_first_extent_item+0x26/0x1f0 [btrfs] Call Trace: <TASK> scrub_find_fill_first_stripe+0x13d/0x3b0 [btrfs] scrub_simple_mirror+0x175/0x260 [btrfs] scrub_stripe+0x5d4/0x6c0 [btrfs] scrub_chunk+0xbb/0x170 [btrfs]	0144da9ab30be42e87e6476638a, https://git.kernel.org/stable/c/6aecd91a5c5b68939cf4169e32bc49f3cd2dd329, https://git.kernel.org/stable/c/aee5f69f3e6cd82bfefaca1b70b40b6cd8f3f784	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scrub_enumerate_chunks+0x2f4/0x5f0 [btrfs] btrfs_scrub_dev+0x240/0x600 [btrfs] btrfs_ioctl+0x1dc8/0x2fa0 [btrfs] ? do_sys_openat2+0xa5/0xf0 __x64_sys_ioctl+0x97/0xc0 do_syscall_64+0x4f/0x120 entry_SYSCALL_64_after_hwframe+0x76/0x7e </TASK> [CAUSE] The reproducer is using a corrupted image where extent tree root is corrupted, thus forcing to use "rescue=all,ro" mount option to mount the image. Then it triggered a scrub, but since scrub relies on extent tree to find where the data/metadata extents are, scrub_find_fill_first_stripe() relies on an non-empty extent root. But unfortunately scrub_find_fill_first_stripe() doesn't really expect an NULL pointer for extent root, it use extent_root to grab fs_info and triggered a NULL pointer dereference. [FIX] Add an extra check for a valid extent root at the beginning of scrub_find_fill_first_stripe(). 		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The new error path is introduced by 42437a6386ff ("btrfs: introduce mount option rescue=ignorebadroots"), but that's pretty old, and later commit b979547513ff ("btrfs: scrub: introduce helper to find and fill sector info for a scrub_stripe") changed how we do scrub. So for kernels older than 6.6, the fix will need manual backport. **CVE ID: CVE-2025-21658**		
Affected Version(s): From (including) 5.14 Up to (excluding) 6.12.10					
NULL Pointer Dereference	19-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net: hns3: fix kernel crash when 1588 is sent on HIP08 devices Currently, HIP08 devices does not register the ptp devices, so the hdev->ptp is NULL. But the tx process would still try to set hardware time stamp info with SKBTX_HW_TSTAMP flag and cause a kernel crash. [128.087798] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000018 ... [128.280251] pc : hclge_ptp_set_tx_info+0x2c/0x140 [hclge] [128.286600] lr : hclge_ptp_set_tx_info+0x20	https://git.kernel.org/stable/c/9741e72b2286de8b38de9db685588ac421a95c87, https://git.kernel.org/stable/c/f19ab3ef96d9626e5f1bdc56d3574c355e83d623	O-LIN-LINU-040225/308

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/0x140 [hclge] [128.292938] sp : ffff800059b93140 [128.297200] x29: ffff800059b93140 x28: 0000000000003280 [128.303455] x27: ffff800020d48280 x26: ffff0cb9dc814080 [128.309715] x25: ffff0cb9cde93fa0 x24: 0000000000000001 [128.315969] x23: 0000000000000000 x22: 0000000000000194 [128.322219] x21: ffff0cd94f986000 x20: 0000000000000000 [128.328462] x19: ffff0cb9d2a166c0 x18: 0000000000000000 [128.334698] x17: 0000000000000000 x16: ffffcf1fc523ed24 [128.340934] x15: 0000ffffd530a518 x14: 0000000000000000 [128.347162] x13: ffff0cd6bdb31310 x12: 0000000000000368 [128.353388] x11: ffff0cb9cfbc7070 x10: ffff2cf55dd11e02 [128.359606] x9 : ffffcf1f85a212b4 x8 : ffff0cd7cf27dab0 [128.365831] x7 : 0000000000000a20 x6 : ffff0cd7cf27d000 [128.372040] x5 : 0000000000000000 x4 : 000000000000ffff [128.378243] x3 : 0000000000000400 x2 : ffffcf1f85a21294 [128.384437] x1 : ffff0cb9db520080 x0 : ffff0cb9db500080 [128.390626] Call trace: [128.393964] hclge_ptp_set_tx_info+0x2c /0x140 [hclge]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[128.399893] hns3_nic_net_xmit+0x39c/0x4c4 [hns3] [128.405468] xmit_one.constprop.0+0xc4/0x200 [128.410600] dev_hard_start_xmit+0x54/0xf0 [128.415556] sch_direct_xmit+0xe8/0x634 [128.420246] __dev_queue_xmit+0x224/0xc70 [128.425101] dev_queue_xmit+0x1c/0x40 [128.429608] ovs_vport_send+0xac/0x1a0 [openvswitch] [128.435409] do_output+0x60/0x17c [openvswitch] [128.440770] do_execute_actions+0x898/0x8c4 [openvswitch] [128.446993] ovs_execute_actions+0x64/0xf0 [openvswitch] [128.453129] ovs_dp_process_packet+0xa0/0x224 [openvswitch] [128.459530] ovs_vport_receive+0x7c/0xfc [openvswitch] [128.465497] internal_dev_xmit+0x34/0xb0 [openvswitch] [128.471460] xmit_one.constprop.0+0xc4/0x200 [128.476561] dev_hard_start_xmit+0x54/0xf0 [128.481489] __dev_queue_xmit+0x968/0xc70 [128.486330] dev_queue_xmit+0x1c/0x40 [128.490856]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ip_finish_output2+0x250/0x570 [128.495810] __ip_finish_output+0x170/0x1e0 [128.500832] ip_finish_output+0x3c/0xf0 [128.505504] ip_output+0xbc/0x160 [128.509654] ip_send_skb+0x58/0xd4 [128.513892] udp_send_skb+0x12c/0x354 [128.518387] udp_sendmsg+0x7a8/0x9c0 [128.522793] inet_sendmsg+0x4c/0x8c [128.527116] __sock_sendmsg+0x48/0x80 [128.531609] __sys_sendto+0x124/0x164 [128.536099] __arm64_sys_sendto+0x30/0x5c [128.540935] invoke_syscall+0x50/0x130 [128.545508] el0_svc_common.constprop.0+0x10c/0x124 [128.551205] do_el0_svc+0x34/0xdc [128.555347] el0_svc+0x20/0x30 [128.559227] el0_sync_handler+0xb8/0xc0 [128.563883] el0_sync+0x160/0x180 **CVE ID: CVE-2025-21649**		
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.124					
Integer Overflow or Wraparound	21-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/081bdb3a31674339313c6d702a	O-LIN-LINU-040225/309

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/sctp: Prevent autoclose integer overflow in sctp_association_init() While by default max_autoclose equals to INT_MAX / HZ, one may set net.sctp.max_autoclose to UINT_MAX. There is code in sctp_association_init() that can consequently trigger overflow. **CVE ID: CVE-2024-57938**	f922bc29de2c53, https://git.kernel.org/stable/c/2297890b778b0e7c8200d6818154f7e461d78e94, https://git.kernel.org/stable/c/271f031f4c31c07e2a85a1ba2b4c8e734909a477	
Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.233					
Integer Overflow or Wraparound	21-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net/sctp: Prevent autoclose integer overflow in sctp_association_init() While by default max_autoclose equals to INT_MAX / HZ, one may set net.sctp.max_autoclose to UINT_MAX. There is code in sctp_association_init() that can consequently trigger overflow. **CVE ID: CVE-2024-57938**	https://git.kernel.org/stable/c/081bdb3a31674339313c6d702af922bc29de2c53, https://git.kernel.org/stable/c/2297890b778b0e7c8200d6818154f7e461d78e94, https://git.kernel.org/stable/c/271f031f4c31c07e2a85a1ba2b4c8e734909a477	O-LIN-LINU-040225/310
Affected Version(s): From (including) 5.7 Up to (excluding) 6.1.125					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: exfat: fix the infinite loop in exfat_readdir() If the file system is corrupted so that a cluster is linked to itself in the cluster chain, and there is an unused directory entry in the cluster, 'dentry' will not be incremented, causing	https://git.kernel.org/stable/c/31beabd0f47f8c3ed9965ba861c9e5b252d4920a, https://git.kernel.org/stable/c/d9ea94f5cd117d56e573696d0045ab3044185a15, https://git.kernel.org/stable/c/dc1d7afceb982e	O-LIN-LINU-040225/311

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition 'dentry < max_dentries' unable to prevent an infinite loop. This infinite loop causes s_lock not to be released, and other tasks will hang, such as exfat_sync_fs(). This commit stops traversing the cluster chain when there is unused directory entry in the cluster to avoid this infinite loop. **CVE ID: CVE-2024-57940**	8f666e70a582e6b5aa806de063	
Affected Version(s): From (including) 6.11 Up to (excluding) 6.12.10					
NULL Pointer Dereference	19-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Fix tlb invalidation when wedging If GuC fails to load, the driver wedges, but in the process it tries to do stuff that may not be initialized yet. This moves the xe_gt_tlb_invalidation_init() to be done earlier: as its own doc says, it's a software-only initialization and should had been named with the _early() suffix. Move it to be called by xe_gt_init_early(), so the locks and seqno are initialized, avoiding a NULL ptr deref when wedging: xe 0000:03:00.0: [drm] *ERROR* GT0: load failed: status: Reset = 0, BootROM = 0x50, UKernel =	https://git.kernel.org/stable/c/09b94ddc58c6640cbbc7775a61a5387b8be71488, https://git.kernel.org/stable/c/9ab4981552930a9c45682d62424ba610edc3992d	O-LIN-LINU-040225/312

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0x00, MIA = 0x00, Auth = 0x01 xe 0000:03:00.0: [drm] *ERROR* GT0: firmware signature verification failed xe 0000:03:00.0: [drm] *ERROR* CRITICAL: Xe has declared device 0000:03:00.0 as wedged. ... BUG: kernel NULL pointer dereference, address: 0000000000000000 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 9 UID: 0 PID: 3908 Comm: modprobe Tainted: G U W 6.13.0-rc4-xe+ #3 Tainted: [U]=USER, [W]=WARN Hardware name: Intel Corporation Alder Lake Client Platform/AlderLake-S ADP-S DDR5 UDIMM CRB, BIOS ADLSFWI1.R00.3275.A00.2207010640 07/01/2022 RIP: 0010:xe_gt_tlb_invalidation_reset+0x75/0x110 [xe] This can be easily triggered by poking the GuC binary to force a signature failure. There will still be an extra message, xe 0000:03:00.0: [drm] *ERROR* GT0: GuC mmio request 0x4100: no reply 0x4100		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			but that's better than a NULL ptr deref. (cherry picked from commit 5001ef3af8f2c972d6fd9c5221a8457556f8bea6) **CVE ID: CVE-2025-21644**		
Affected Version(s): From (including) 6.12 Up to (excluding) 6.12.10					
NULL Pointer Dereference	19-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: usb: typec: tcpci: fix NULL pointer issue on shared irq case The tcpci_irq() may meet below NULL pointer dereference issue: [2.641851] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000010 [2.641951] status 0x1, 0x37f [2.650659] Mem abort info: [2.656490] ESR = 0x0000000096000004 [2.660230] EC = 0x25: DABT (current EL), IL = 32 bits [2.665532] SET = 0, FnV = 0 [2.668579] EA = 0, S1PTW = 0 [2.671715] FSC = 0x04: level 0 translation fault [2.676584] Data abort info: [2.679459] ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 [2.684936] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [2.689980] GCS = 0, Overlay = 0, DirtyBit = 0, Xs	https://git.kernel.org/stable/c/8586d6ea623e48b2bd38304bbc52b0b8228816ff, https://git.kernel.org/stable/c/862a9c0f68487fd6ced15622d9cdcec48f8b5aaa	O-LIN-LINU-040225/313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			= 0 [2.695284] [0000000000000010] user address but active_mm is swapper [2.701632] Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP [2.707883] Modules linked in: [2.710936] CPU: 1 UID: 0 PID: 87 Comm: irq/111-2-0051 Not tainted 6.12.0-rc6-06316-g7f63786ad3d1-dirty #4 [2.720570] Hardware name: NXP i.MX93 11X11 EVK board (DT) [2.726040] pstate: 60400009 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) [2.732989] pc : tcpci_irq+0x38/0x318 [2.736647] lr : _tcpci_irq+0x14/0x20 [2.740295] sp : ffff80008324bd30 [2.743597] x29: ffff80008324bd70 x28: ffff800080107894 x27: ffff800082198f70 [2.750721] x26: ffff0000050e6680 x25: ffff000004d172ac x24: ffff0000050f0000 [2.757845] x23: ffff000004d17200 x22: 0000000000000001 x21: ffff0000050f0000 [2.764969] x20: ffff000004d17200 x19: 0000000000000000 x18: 0000000000000001 [2.772093] x17: 0000000000000000 x16: ffff80008183d8a0 x15: ffff00007fbab040 [2.779217] x14: ffff00007fb918c0 x13: 0000000000000000 x12: 000000000000017a		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[2.786341] x11: 0000000000000001 x10: 0000000000000a90 x9 : ffff80008324bd00 [2.793465] x8 : ffff0000050f0af0 x7 : ffff00007fbaa840 x6 : 0000000000000031 [2.800589] x5 : 000000000000017a x4 : 0000000000000002 x3 : 0000000000000002 [2.807713] x2 : ffff80008324bd3a x1 : 0000000000000010 x0 : 0000000000000000 [2.814838] Call trace: [2.817273] tcpci_irq+0x38/0x318 [2.820583] _tcpci_irq+0x14/0x20 [2.823885] irq_thread_fn+0x2c/0xa8 [2.827456] irq_thread+0x16c/0x2f4 [2.830940] kthread+0x110/0x114 [2.834164] ret_from_fork+0x10/0x20 [2.837738] Code: f9426420 f9001fe0 d2800000 52800201 (f9400a60) This may happen on shared irq case. Such as two Type-C ports share one irq. After the first port finished tcpci_register_port(), it may trigger interrupt. However, if the interrupt comes by chance the 2nd port finishes devm_request_threaded_irq(), the 2nd port interrupt handler will run at first. Then the above issue happens due to tcpci is still a NULL pointer in tcpci_irq() when dereference to regmap.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devm_request_threaded_irq() <-- port1 irq comes disable_irq(client->irq); tcpci_register_port() This will restore the logic to the state before commit (77e85107a771 "usb: typec: tcpci: support edge irq"). However, moving tcpci_register_port() earlier creates a problem when use edge irq because tcpci_init() will be called before devm_request_threaded_irq(). The tcpci_init() writes the ALERT_MASK to the hardware to tell it to start generating interrupts but we're not ready to deal with them yet, then the ALERT events may be missed and ALERT line will not recover to high level forever. To avoid the issue, this will also set ALERT_MASK register after devm_request_threaded_irq() return. **CVE ID: CVE-2024-57914**		
NULL Pointer Dereference	19-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: nfs: Fix oops in nfs_netfs_init_request() when copying to cache When netfslib wants to copy some data that has just been read on behalf of nfs, it creates a new write	https://git.kernel.org/stable/c/13a07cc81e2d116cece727a83746c74b87a9d417, https://git.kernel.org/stable/c/86ad1a58f6a9453f49e06ef957a40a8dac00a13f	O-LIN-LINU-040225/314

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request and calls nfs_netfs_init_request() to initialise it, but with a NULL file pointer. This causes nfs_file_open_context() to oops - however, we don't actually need the nfs context as we're only going to write to the cache. Fix this by just returning if we aren't given a file pointer and emit a warning if the request was for something other than copy-to-cache. Further, fix nfs_netfs_free_request() so that it doesn't try to free the context if the pointer is NULL. **CVE ID: CVE-2024-57927**		
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.70					
Integer Overflow or Wraparound	21-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net/sctp: Prevent autoclose integer overflow in sctp_association_init() While by default max_autoclose equals to INT_MAX / HZ, one may set net.sctp.max_autoclose to UINT_MAX. There is code in sctp_association_init() that can consequently trigger overflow. **CVE ID: CVE-2024-57938**	https://git.kernel.org/stable/c/081bdb3a31674339313c6d702af922bc29de2c53, https://git.kernel.org/stable/c/2297890b778b0e7c8200d6818154f7e461d78e94, https://git.kernel.org/stable/c/271f031f4c31c07e2a85a1ba2b4c8e734909a477	O-LIN-LINU-040225/315
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.72					
NULL Pointer Dereference	19-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: u_serial: Disable ep before setting	https://git.kernel.org/stable/c/0c50f00cc29948184af05bda31392fff5821f4f3, https://git.kern	O-LIN-LINU-040225/316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			port to null to fix the crash caused by port being null Considering that in some extreme cases, when performing the unbinding operation, gserial_disconnect has cleared gser->ioport, which triggers gadget reconfiguration, and then calls gs_read_complete, resulting in access to a null pointer. Therefore, ep is disabled before gserial_disconnect sets port to null to prevent this from happening. Call trace: gs_read_complete+0x58/0x240 usb_gadget_giveback_request+0x40/0x160 dwc3_remove_requests+0x170/0x484 dwc3_ep0_out_start+0xb0/0x1d4 __dwc3_gadget_start+0x25c/0x720 kretprobe_trampoline.cfi_jt+0x0/0x8 kretprobe_trampoline.cfi_jt+0x0/0x8 udc_bind_to_driver+0x1d8/0x300 usb_gadget_probe_driver+0xa8/0x1dc gadget_dev_desc_UDC_store+0x13c/0x188 configfs_write_iter+0x160/	el.org/stable/c/13014969cbf07f18d62ceea40bd8ca8ec9d36cec, https://git.kernel.org/stable/c/3d730e8758c75b68a0152ee1ac48a270ea6725b4	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0x1f4 vfs_write+0x2d0/0x40c ksys_write+0x7c/0xf0 __arm64_sys_write+0x20/0x30 invoke_syscall+0x60/0x150 el0_svc_common+0x8c/0xf8 do_el0_svc+0x28/0xa0 el0_svc+0x24/0x84 **CVE ID: CVE-2024-57915**		
Loop with Unreachable Exit Condition ('Infinite Loop')	21-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: exfat: fix the infinite loop in exfat_readdir() If the file system is corrupted so that a cluster is linked to itself in the cluster chain, and there is an unused directory entry in the cluster, 'dentry' will not be incremented, causing condition 'dentry < max_dentries' unable to prevent an infinite loop. This infinite loop causes s_lock not to be released, and other tasks will hang, such as exfat_sync_fs(). This commit stops traversing the cluster chain when there is unused directory entry in the cluster to avoid this infinite loop. **CVE ID: CVE-2024-57940**	https://git.kernel.org/stable/c/31beabd0f47f8c3ed9965ba861c9e5b252d4920a, https://git.kernel.org/stable/c/d9ea94f5cd117d56e573696d0045ab3044185a15, https://git.kernel.org/stable/c/dc1d7afceb982e8f666e70a582e6b5aa806de063	O-LIN-LINU-040225/317

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 6.4 Up to (excluding) 6.6.70					
NULL Pointer Dereference	21-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: gve: guard XSK operations on the existence of queues This patch predicates the enabling and disabling of XSK pools on the existence of queues. As it stands, if the interface is down, disabling or enabling XSK pools would result in a crash, as the RX queue pointer would be NULL. XSK pool registration will occur as part of the next interface up. Similarly, xsk_wakeup needs be guarded against queues disappearing while the function is executing, so a check against the GVE_PRIV_FLAGS_NAPI_ENABLED flag is added to synchronize with the disabling of the bit and the synchronize_net() in gve_turndown. **CVE ID: CVE-2024-57933**	https://git.kernel.org/stable/c/40338d7987d810fcaa95c500b1068a52b08eec9b, https://git.kernel.org/stable/c/771d66f2bd8c4dba1286a9163ab982cecd825718, https://git.kernel.org/stable/c/8e8d7037c89437af12725f454e2eaf40e8166c0f	O-LIN-LINU-040225/318
Affected Version(s): From (including) 6.4 Up to (excluding) 6.6.72					
Use After Free	19-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/mediatek: Set private->all_drm_private[i]->drm to NULL if mtk_drm_bind returns err The pointer need to be set to NULL, otherwise KASAN complains about use-after-free. Because in	https://git.kernel.org/stable/c/078b2ff7da200b7532398e668eef723ad40fb516, https://git.kernel.org/stable/c/36684e9d88a2e2401ae26715a2e217cb4295cea7, https://git.kernel.org/stable/c/	O-LIN-LINU-040225/319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mtk_drm_bind, all private's drm are set as follows. private->all_drm_private[i]->drm = drm; And drm will be released by drm_dev_put in case mtk_drm_kms_init returns failure. However, the shutdown path still accesses the previous allocated memory in drm_atomic_helper_shutdown. [84.874820] watchdog: watchdog0: watchdog did not stop! [86.512054] ========== [86.513162] BUG: KASAN: use-after-free in drm_atomic_helper_shutdown+0x33c/0x378 [86.514258] Read of size 8 at addr ffff0000d46fc068 by task shutdown/1 [86.515213] [86.515455] CPU: 1 UID: 0 PID: 1 Comm: shutdown Not tainted 6.13.0-rc1-mtk+gfa1a78e5d24b-dirty #55 [86.516752] Hardware name: Unknown Product/Unknown Product, BIOS 2022.10 10/01/2022 [86.517960] Call trace: [86.518333] show_stack+0x20/0x38 (C) [86.518891] dump_stack_lvl+0x90/0xd0 [86.519443]	7083b93e9755d60f0c2bcaa9d064308108280534	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			print_report+0xf8/0x5b0 [86.519985] kasan_report+0xb4/0x100 [86.520526] __asan_report_load8_noabort+0x20/0x30 [86.521240] drm_atomic_helper_shutdown+0x33c/0x378 [86.521966] mtk_drm_shutdown+0x54/0x80 [86.522546] platform_shutdown+0x64/0x90 [86.523137] device_shutdown+0x260/0x5b8 [86.523728] kernel_restart+0x78/0xf0 [86.524282] __do_sys_reboot+0x258/0x2f0 [86.524871] __arm64_sys_reboot+0x90/0xd8 [86.525473] invoke_syscall+0x74/0x268 [86.526041] el0_svc_common.constprop.0+0xb0/0x240 [86.526751] do_el0_svc+0x4c/0x70 [86.527251] el0_svc+0x4c/0xc0 [86.527719] el0t_64_sync_handler+0x144/0x168 [86.528367] el0t_64_sync+0x198/0x1a0 [86.528920] [86.529157] The buggy address belongs to the physical page: [86.529972] page: refcount:0 mapcount:0 mapping:0000000000000000 index:0xffff0000d46fd4d0 pfn:0x1146fc		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[86.531319] flags: 0xbfffc0000000000(node=0|zone=2|lastcpupid=0xffff) [86.532267] raw: 0bfffc0000000000 0000000000000000 dead000000000122 0000000000000000 [86.533390] raw: ffff0000d46fd4d0 0000000000000000 00000000ffffffff 0000000000000000 [86.534511] page dumped because: kasan: bad access detected [86.535323] [86.535559] Memory state around the buggy address: [86.536265] ffff0000d46fbf00: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff [86.537314] ffff0000d46fbf80: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff [86.538363] >ffff0000d46fc000: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff [86.544733] ^ [86.551057] ffff0000d46fc080: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff [86.557510] ffff0000d46fc100: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff [86.563928] ========== [86.571093] Disabling lock debugging due to kernel taint [86.577642] Unable to handle kernel paging request at virtual address e0e9c0920000000b [86.581834] KASAN: maybe wild-memory-		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access in range [0x0752049000000058-0x075204900000005f] ... **CVE ID: CVE-2024-57926**		
Affected Version(s): From (including) 6.7 Up to (excluding) 6.12.10					
Use After Free	19-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/mediatek: Set private->all_drm_private[i]->drm to NULL if mtk_drm_bind returns err The pointer need to be set to NULL, otherwise KASAN complains about use-after-free. Because in mtk_drm_bind, all private's drm are set as follows. private->all_drm_private[i]->drm = drm; And drm will be released by drm_dev_put in case mtk_drm_kms_init returns failure. However, the shutdown path still accesses the previous allocated memory in drm_atomic_helper_shutdown. [84.874820] watchdog: watchdog0: watchdog did not stop! [86.512054] ========== [86.513162] BUG: KASAN: use-after-free in drm_atomic_helper_shutdown+0x33c/0x378	https://git.kernel.org/stable/c/078b2ff7da200b7532398e668eef723ad40fb516, https://git.kernel.org/stable/c/36684e9d88a2e2401ae26715a2e217cb4295cea7, https://git.kernel.org/stable/c/7083b93e9755d60f0c2bcaa9d064308108280534	O-LIN-LINU-040225/320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[86.514258] Read of size 8 at addr ffff0000d46fc068 by task shutdown/1 [86.515213] [86.515455] CPU: 1 UID: 0 PID: 1 Comm: shutdown Not tainted 6.13.0-rc1-mtk+gfa1a78e5d24b-dirty #55 [86.516752] Hardware name: Unknown Product/Unknown Product, BIOS 2022.10 10/01/2022 [86.517960] Call trace: [86.518333] show_stack+0x20/0x38 (C) [86.518891] dump_stack_lvl+0x90/0xd0 [86.519443] print_report+0xf8/0x5b0 [86.519985] kasan_report+0xb4/0x100 [86.520526] __asan_report_load8_noabort+0x20/0x30 [86.521240] drm_atomic_helper_shutdown+0x33c/0x378 [86.521966] mtk_drm_shutdown+0x54/0x80 [86.522546] platform_shutdown+0x64/0x90 [86.523137] device_shutdown+0x260/0x5b8 [86.523728] kernel_restart+0x78/0xf0 [86.524282] __do_sys_reboot+0x258/0x2f0 [86.524871] __arm64_sys_reboot+0x90/0xd8 [86.525473] invoke_syscall+0x74/0x268 [86.526041] el0_svc_common.constprop		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			.0+0xb0/0x240 [86.526751] do_el0_svc+0x4c/0x70 [86.527251] el0_svc+0x4c/0xc0 [86.527719] el0t_64_sync_handler+0x144/0x168 [86.528367] el0t_64_sync+0x198/0x1a0 [86.528920] [86.529157] The buggy address belongs to the physical page: [86.529972] page: refcount:0 mapcount:0 mapping:0000000000000000 index:0xffff0000d46fd4d0 pfn:0x1146fc [86.531319] flags: 0xbfffc0000000000(node=0|zone=2|lastcpupid=0xffff) [86.532267] raw: 0bfffc0000000000 0000000000000000 dead000000000122 0000000000000000 [86.533390] raw: ffff0000d46fd4d0 0000000000000000 00000000ffffffff 0000000000000000 [86.534511] page dumped because: kasan: bad access detected [86.535323] [86.535559] Memory state around the buggy address: [86.536265] ffff0000d46fbf00: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff [86.537314] ffff0000d46fbf80: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff [86.538363] >ffff0000d46fc000: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff [86.544733]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			^ [86.551057] ffff0000d46fc080: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff [86.557510] ffff0000d46fc100: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff [86.563928] ========== [86.571093] Disabling lock debugging due to kernel taint [86.577642] Unable to handle kernel paging request at virtual address e0e9c0920000000b [86.581834] KASAN: maybe wild-memory-access in range [0x0752049000000058-0x075204900000005f] ... **CVE ID: CVE-2024-57926**		
Loop with Unreachable Exit Condition ('Infinite Loop')	21-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: exfat: fix the infinite loop in exfat_readdir() If the file system is corrupted so that a cluster is linked to itself in the cluster chain, and there is an unused directory entry in the cluster, 'dentry' will not be incremented, causing condition 'dentry < max_dentries' unable to prevent an infinite loop. This infinite loop causes s_lock not to be released, and other	https://git.kernel.org/stable/c/31beabd0f47f8c3ed9965ba861c9e5b252d4920a, https://git.kernel.org/stable/c/d9ea94f5cd117d56e573696d0045ab3044185a15, https://git.kernel.org/stable/c/dc1d7afceb982e8f666e70a582e6b5aa806de063	O-LIN-LINU-040225/321

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tasks will hang, such as exfat_sync_fs(). This commit stops traversing the cluster chain when there is unused directory entry in the cluster to avoid this infinite loop. **CVE ID: CVE-2024-57940**		
NULL Pointer Dereference	21-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: avoid NULL pointer dereference if no valid extent tree [BUG] Syzbot reported a crash with the following call trace: BTRFS info (device loop0): scrub: started on devid 1 BUG: kernel NULL pointer dereference, address: 0000000000000208 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 106e70067 P4D 106e70067 PUD 107143067 PMD 0 Oops: Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 1 UID: 0 PID: 689 Comm: repro Kdump: loaded Tainted: G O 6.13.0-rc4-custom+ #206 Tainted: [O]=OOT_MODULE Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS unknown 02/02/2022 RIP: 0010:find_first_extent_item +0x26/0x1f0 [btrfs]	https://git.kernel.org/stable/c/24b85a8b0310e0144da9ab30be42e87e6476638a, https://git.kernel.org/stable/c/6aecd91a5c5b68939cf4169e32bc49f3cd2dd329, https://git.kernel.org/stable/c/aee5f69f3e6cd82bfefaca1b70b40b6cd8f3f784	O-LIN-LINU-040225/322

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Call Trace: <TASK> scrub_find_fill_first_stripe+0x13d/0x3b0 [btrfs] scrub_simple_mirror+0x175/0x260 [btrfs] scrub_stripe+0x5d4/0x6c0 [btrfs] scrub_chunk+0xbb/0x170 [btrfs] scrub_enumerate_chunks+0x2f4/0x5f0 [btrfs] btrfs_scrub_dev+0x240/0x600 [btrfs] btrfs_ioctl+0x1dc8/0x2fa0 [btrfs] ? do_sys_openat2+0xa5/0xf0 __x64_sys_ioctl+0x97/0xc0 do_syscall_64+0x4f/0x120 entry_SYSCALL_64_after_hwframe+0x76/0x7e </TASK> [CAUSE] The reproducer is using a corrupted image where extent tree root is corrupted, thus forcing to use "rescue=all,ro" mount option to mount the image. Then it triggered a scrub, but since scrub relies on extent tree to find where the data/metadata extents are, scrub_find_fill_first_stripe() relies on an non-empty extent root.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			But unfortunately scrub_find_fill_first_stripe() doesn't really expect an NULL pointer for extent root, it use extent_root to grab fs_info and triggered a NULL pointer dereference. [FIX] Add an extra check for a valid extent root at the beginning of scrub_find_fill_first_stripe() . The new error path is introduced by 42437a6386ff ("btrfs: introduce mount option rescue=ignorebadroots"), but that's pretty old, and later commit b979547513ff ("btrfs: scrub: introduce helper to find and fill sector info for a scrub_stripe") changed how we do scrub. So for kernels older than 6.6, the fix will need manual backport. **CVE ID: CVE-2025-21658**		
NULL Pointer Dereference	19-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: u_serial: Disable ep before setting port to null to fix the crash caused by port being null Considering that in some extreme cases, when performing the unbinding operation, gserial_disconnect has cleared gser->ioport,	https://git.kernel.org/stable/c/0c50f00cc29948184af05bda31392fff5821f4f3, https://git.kernel.org/stable/c/13014969cbf07f18d62ceea40bd8ca8ec9d36cec, https://git.kernel.org/stable/c/3d730e8758c75b68a0152ee1ac	O-LIN-LINU-040225/323

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which triggers gadget reconfiguration, and then calls gs_read_complete, resulting in access to a null pointer. Therefore, ep is disabled before gserial_disconnect sets port to null to prevent this from happening. Call trace: gs_read_complete+0x58/0x240 usb_gadget_giveback_request+0x40/0x160 dwc3_remove_requests+0x170/0x484 dwc3_ep0_out_start+0xb0/0x1d4 __dwc3_gadget_start+0x25c/0x720 kretprobe_trampoline.cfi_jt+0x0/0x8 kretprobe_trampoline.cfi_jt+0x0/0x8 udc_bind_to_driver+0x1d8/0x300 usb_gadget_probe_driver+0xa8/0x1dc gadget_dev_desc_UDC_store+0x13c/0x188 configfs_write_iter+0x160/0x1f4 vfs_write+0x2d0/0x40c ksys_write+0x7c/0xf0 __arm64_sys_write+0x20/0x30 invoke_syscall+0x60/0x150	48a270ea6725b4	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			el0_svc_common+0x8c/0xf8 do_el0_svc+0x28/0xa0 el0_svc+0x24/0x84 **CVE ID: CVE-2024-57915**		
Affected Version(s): From (including) 6.7 Up to (excluding) 6.12.9					
Integer Overflow or Wraparound	21-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net/sctp: Prevent autoclose integer overflow in sctp_association_init() While by default max_autoclose equals to INT_MAX / HZ, one may set net.sctp.max_autoclose to UINT_MAX. There is code in sctp_association_init() that can consequently trigger overflow. **CVE ID: CVE-2024-57938**	https://git.kernel.org/stable/c/081bdb3a31674339313c6d702af922bc29de2c53, https://git.kernel.org/stable/c/2297890b778b0e7c8200d6818154f7e461d78e94, https://git.kernel.org/stable/c/271f031f4c31c07e2a85a1ba2b4c8e734909a477	O-LIN-LINU-040225/324
NULL Pointer Dereference	21-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: gve: guard XSK operations on the existence of queues This patch predicates the enabling and disabling of XSK pools on the existence of queues. As it stands, if the interface is down, disabling or enabling XSK pools would result in a crash, as the RX queue pointer would be NULL. XSK pool registration will occur as part of the next interface up. Similarly, xsk_wakeup needs be guarded against queues disappearing while the function is	https://git.kernel.org/stable/c/40338d7987d810fcaa95c500b1068a52b08eec9b, https://git.kernel.org/stable/c/771d66f2bd8c4dba1286a9163ab982cecd825718, https://git.kernel.org/stable/c/8e8d7037c89437af12725f454e2eaf40e8166c0f	O-LIN-LINU-040225/325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executing, so a check against the GVE_PRIV_FLAGS_NAPI_ENABLED flag is added to synchronize with the disabling of the bit and the synchronize_net() in gve_turndown. **CVE ID: CVE-2024-57933**		
Affected Version(s): From (including) 6.9 Up to (excluding) 6.12.10					
NULL Pointer Dereference	21-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: iio: adc: ti-ads1298: Add NULL check in ads1298_init devm_kasprintf() can return a NULL pointer on failure. A check on the return value of such a call in ads1298_init() is missing. Add it. **CVE ID: CVE-2024-57944**	https://git.kernel.org/stable/c/69b680bbac9bd611aaa308769d6c71e3e70eb3c3, https://git.kernel.org/stable/c/bcb394bb28e55312cace75362b8e489eb0e02a30	O-LIN-LINU-040225/326
Vendor: Sonicwall					
Product: sma6200_firmware					
Affected Version(s): * Up to (excluding) 12.4.3-02854					
Deserialization of Untrusted Data	23-Jan-2025	9.8	Pre-authentication deserialization of untrusted data vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC), which in specific conditions could potentially enable a remote unauthenticated attacker to execute arbitrary OS commands. **CVE ID: CVE-2025-23006**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002	O-SON-SMA6-040225/327
Product: sma6210_firmware					
Affected Version(s): * Up to (excluding) 12.4.3-02854					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	23-Jan-2025	9.8	Pre-authentication deserialization of untrusted data vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC), which in specific conditions could potentially enable a remote unauthenticated attacker to execute arbitrary OS commands. **CVE ID: CVE-2025-23006**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002	O-SON-SMA6-040225/328
Product: sma7200_firmware					
Affected Version(s): * Up to (excluding) 12.4.3-02854					
Deserialization of Untrusted Data	23-Jan-2025	9.8	Pre-authentication deserialization of untrusted data vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC), which in specific conditions could potentially enable a remote unauthenticated attacker to execute arbitrary OS commands. **CVE ID: CVE-2025-23006**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002	O-SON-SMA7-040225/329
Product: sma7210_firmware					
Affected Version(s): * Up to (excluding) 12.4.3-02854					
Deserialization of Untrusted Data	23-Jan-2025	9.8	Pre-authentication deserialization of untrusted data vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC), which in specific conditions could potentially enable a remote unauthenticated attacker to execute arbitrary OS commands. **CVE ID: CVE-2025-23006**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002	O-SON-SMA7-040225/330

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sra_ex6000_firmware					
Affected Version(s): * Up to (including) 12.4.3-02804					
Deserialization of Untrusted Data	23-Jan-2025	9.8	Pre-authentication deserialization of untrusted data vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC), which in specific conditions could potentially enable a remote unauthenticated attacker to execute arbitrary OS commands. **CVE ID: CVE-2025-23006**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002	O-SON-SRA_-040225/331
Product: sra_ex7000_firmware					
Affected Version(s): * Up to (including) 12.4.3-02804					
Deserialization of Untrusted Data	23-Jan-2025	9.8	Pre-authentication deserialization of untrusted data vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC), which in specific conditions could potentially enable a remote unauthenticated attacker to execute arbitrary OS commands. **CVE ID: CVE-2025-23006**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002	O-SON-SRA_-040225/332
Product: sra_ex9000_firmware					
Affected Version(s): * Up to (including) 12.4.3-02804					
Deserialization of Untrusted Data	23-Jan-2025	9.8	Pre-authentication deserialization of untrusted data vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC), which in specific conditions could potentially enable a remote unauthenticated attacker to	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002	O-SON-SRA_-040225/333

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary OS commands. **CVE ID: CVE-2025-23006**		
Vendor: Tenda					
Product: ac18_firmware					
Affected Version(s): 15.03.05.19					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Jan-2025	9.8	Tenda AC18 V15.03.05.19 was discovered to contain a command injection vulnerability via the usbName parameter in the formSetSambaConf function. **CVE ID: CVE-2024-57583**	N/A	O-TEN-AC18-040225/334
Out-of-bounds Write	16-Jan-2025	9.8	Tenda AC18 V15.03.05.19 was discovered to contain a stack overflow via the ssid parameter in the form_fast_setting_wifi_set function. **CVE ID: CVE-2024-57575**	N/A	O-TEN-AC18-040225/335

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions