National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
16 – 30 Jun 2024 Vol. 11 No. 12
https://nciipc.gov.in/

Table of Content

Vendor	Product	Page Number
Omron	nj501-4320_firmware	434
	nj501-4400_firmware	435
	nj501-4500_firmware	435
	nj501-5300-1_firmware	436
	nj501-5300_firmware	436
	nj501-r300_firmware	436
	nj501-r320_firmware	437
	nj501-r400_firmware	437
	nj501-r420_firmware	438
	nj501-r500_firmware	438
	nj501-r520_firmware	439
	nx102-1000_firmware	439
	nx102-1020_firmware	440
	nx102-1100_firmware	440
	nx102-1120_firmware	440
	nx102-1200_firmware	441
	nx102-1220_firmware	441
	nx102-9000_firmware	442
	nx102-9020_firmware	442
	nx1p2-1040dt1_firmware	443
	nx1p2-1040dt_firmware	443
	nx1p2-1140dt1_firmware	444
	nx1p2-1140dt_firmware	444
	nx1p2-9024dt1_firmware	444
	nx1p2-9024dt_firmware	445
	nx1w-adb21_firmware	445
	nx1w-cif01_firmware	446
	nx1w-cif11_firmware	446
	nx1w-cif12_firmware	447
	nx1w-dab21v_firmware	447
	nx1w-mab221_firmware	448
	nx701-1600_firmware	448

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 5starplugins					
Product: easy_age_verify					
Affected Version(s): * Up to (excluding) 1.8.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-2024	4.8	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in 5 Star Plugins Easy Age Verify allows Stored XSS.This issue affects Easy Age Verify: from n/a through 1.8.2. **CVE ID: CVE-2024-35757**	N/A	A-5ST-EASY-100724/1
Vendor: access_management_specialist_project					
Product: access_management_specialist					
Affected Version(s): 6.62.51215					
N/A	24-Jun-2024	7.5	An issue in Shenzhen Weitillage Industrial Co., Ltd the access management specialist V6.62.51215 allows a remote attacker to obtain sensitive information. **CVE ID: CVE-2024-37677**	N/A	A-ACC-ACCE-100724/2
Vendor: adminerevo					
Product: adminerevo					

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) 4.8.3					
Unrestricted Upload of File with Dangerous Type	21-Jun-2024	9.8	The file upload plugin in Adminer and AdminerEvo allows an attacker to upload a file with a table name of ".." to the root of the Adminer directory. The attacker can effectively guess the name of the uploaded file and execute it. Adminer is no longer supported, but this issue was fixed in AdminerEvo version 4.8.3. **CVE ID: CVE-2023-45197**	https://github.com/adminerevo/adminerevo/commit/1cc06d6a1005fd833fa009701badd5641627a1d4	A-ADM-ADMI-100724/3
Vendor: admiror-design-studio					
Product: admirorframes					
Affected Version(s): * Up to (excluding) 5.0					
N/A	28-Jun-2024	7.5	Full Path Disclosure vulnerability in AdmirorFrames Joomla! extension in afHelper.php script allows an unauthorised attacker to retrieve location of web root folder. This issue affects AdmirorFrames: before 5.0. **CVE ID: CVE-2024-5735**	N/A	A-ADM-ADMI-100724/4
Server-Side	28-Jun-2024	7.5	Server Side Request Forgery (SSRF)	N/A	A-ADM-ADMI-100724/5

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 Forgery (SSRF)			vulnerability in AdmirorFrames Joomla! extension in afGdStream.php script allows to access local files or server pages available only from localhost. This issue affects AdmirorFrames: before 5.0. **CVE ID: CVE-2024-5736**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jun-2024	6.1	Script afGdStream.php in AdmirorFrames Joomla! extension doesn't specify a content type and as a result default (text/html) is used. An attacker may embed HTML tags directly in image data which is rendered by a webpage as HTML. This issue affects AdmirorFrames: before 5.0. **CVE ID: CVE-2024-5737**	N/A	A-ADM-ADMI-100724/6
Vendor: ali2woo					
Product: ali2woo					
Affected Version(s): * Up to (including) 3.3.5					
Cross-Site Request Forgery (CSRF)	21-Jun-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Ali2Woo Ali2Woo Lite.This issue	N/A	A-ALI-ALI2-100724/7

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
			affects Ali2Woo Lite: from n/a through 3.3.5. **CVE ID: CVE-2024-37212**		
Vendor: Amazon					
Product: freertos-plus-tcp					
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.1.1					
Out-of-bounds Read	24-Jun-2024	8.1	FreeRTOS-Plus-TCP is a lightweight TCP/IP stack for FreeRTOS. FreeRTOS-Plus-TCP versions 4.0.0 through 4.1.0 contain a buffer over-read issue in the DNS Response Parser when parsing domain names in a DNS response. A carefully crafted DNS response with domain name length value greater than the actual domain name length, could cause the parser to read beyond the DNS response buffer. This issue affects applications using DNS functionality of the FreeRTOS-Plus-TCP stack. Applications that do not use DNS functionality are not affected, even when the DNS	https://github.com/FreeRTOS/FreeRTOS-Plus-TCP/security/advisories/GHSA-ppcp-rg65-58mv	A-AMA-FREE-100724/8

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
			functionality is enabled. This vulnerability has been patched in version 4.1.1. **CVE ID: CVE-2024-38373**		
Vendor: Anchorcms					
Product: anchor_cms					
Affected Version(s): 0.12.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jun-2024	6.1	Cross Site Scripting vulnerability in Anchor CMS v.0.12.7 allows a remote attacker to execute arbitrary code via a crafted .pdf file. **CVE ID: CVE-2024-37732**	N/A	A-ANC-ANCH-100724/9
Vendor: artbees					
Product: jupiter_x_core					
Affected Version(s): * Up to (including) 3.3.8					
Incorrect Authorization	21-Jun-2024	9.8	Incorrect Authorization vulnerability in Artbees JupiterX Core allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects JupiterX Core: from n/a through 3.3.8. **CVE ID: CVE-2023-38389**	N/A	A-ART-JUPI-100724/10
Vendor: auto-featured-image_project					

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: auto-featured-image					
Affected Version(s): * Up to (including) 1.2					
Unrestricted Upload of File with Dangerous Type	27-Jun-2024	8.8	The Auto Featured Image plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'create_post_attachment_from_url' function in all versions up to, and including, 1.2. This makes it possible for authenticated attackers, with contributor-level and above permissions, to upload arbitrary files on the affected site's server which may make remote code execution possible. **CVE ID: CVE-2024-6054**	N/A	A-AUT-AUTO-100724/11
Vendor: averta					
Product: master_slider					
Affected Version(s): * Up to (including) 3.9.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jun-2024	5.4	The Master Slider – Responsive Touch Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ms_layer' shortcode in all versions up to, and	N/A	A-AVE-MAST-100724/12

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
			including, 3.9.10 due to insufficient input sanitization and output escaping on the 'css_id' user supplied attribute. 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-2024-4375**		
Vendor: awplife					
Product: event_monster					
Affected Version(s): * Up to (including) 1.4.0					
N/A	21-Jun-2024	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in A WP Life Event Management Tickets Booking.This issue affects Event Management Tickets Booking: from n/a through 1.4.0. **CVE ID: CVE-2024-5059**	N/A	A-AWP-EVEN-100724/13
Vendor: back2nature					
Product: word_balloon					

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 (including) 4.21.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Jun-2024	6.5	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in YAHMAN Word Balloon allows PHP Local File Inclusion.This issue affects Word Balloon: from n/a through 4.21.1. **CVE ID: CVE-2024-35781**	N/A	A-BAC-WORD-100724/14
Vendor: billminozzi					
Product: wp_tools					
Affected Version(s): * Up to (excluding) 3.43					
Missing Authorization	21-Jun-2024	8.8	Missing Authorization vulnerability in Bill Minozzi WP Tools.This issue affects WP Tools: from n/a through 3.41. **CVE ID: CVE-2022-43453**	N/A	A-BIL-WP_T-100724/15
Vendor: blazethemes					
Product: digital_newspaper					
Affected Version(s): * Up to (excluding) 1.1.6					
Cross-Site Request Forgery (CSRF)	21-Jun-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in blazethemes Digital Newspaper.This issue affects Digital	N/A	A-BLA-DIGI-100724/16

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Newspaper: from n/a through 1.1.5. **CVE ID: CVE-2024-37198**		
Vendor: bricksbuilder					
Product: bricks					
Affected Version(s): * Up to (excluding) 1.9.9					
Authorization Bypass Through User-Controlled Key	22-Jun-2024	4.3	The Bricks Builder plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.9.8 via the postId parameter due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Contributor-level access and above, to modify posts and pages created by other users including admins. As a requirement for this, an admin would have to enable access to the editor specifically for such a user or enable it for all users with a certain user account type. **CVE ID: CVE-2024-4874**	N/A	A-BRI-BRIC-100724/17
Vendor: businessdirectoryplugin					

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: business_directory					
Affected Version(s): * Up to (excluding) 6.4.4					
Improper Neutralization of Formula Elements in a CSV File	18-Jun-2024	8	The Business Directory Plugin plugin for WordPress is vulnerable to CSV Injection in versions up to, and including, 6.4.3 via the class-csv-exporter.php file. This allows authenticated attackers, with author-level permissions and above, to embed untrusted input into CSV files exported by administrators, which can result in code execution when these files are downloaded and opened on a local system with a vulnerable configuration. **CVE ID: CVE-2023-5527**	N/A	A-BUS-BUSI-100724/18
Vendor: church_admin_project					
Product: church_admin					
Affected Version(s): * Up to (excluding) 4.4.5					
Improper Neutralization of Input During Web Page Generation	21-Jun-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Andy Moyle Church	N/A	A-CHU-CHUR-100724/19

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
('Cross-site Scripting')			Admin allows Stored XSS.This issue affects Church Admin: from n/a through 4.4.4. **CVE ID: CVE-2024-35764**		
Vendor: conceptintermedia					
Product: s\@m_cms					
Affected Version(s): * Up to (including) 3.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Jun-2024	9.8	Sites managed in S@M CMS (Concept Intermedia) might be vulnerable to a blind SQL Injection executed using the search bar. Only a part of observed services is vulnerable, but since vendor has not investigated the root problem, it is hard to determine when the issue appears. **CVE ID: CVE-2024-3816**	N/A	A-CON-S\@M-100724/20
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jun-2024	6.1	Sites managed in S@M CMS (Concept Intermedia) might be vulnerable to Reflected XSS via including scripts in requested file names. Only a part of observed services is vulnerable, but since vendor has not investigated the	N/A	A-CON-S\@M-100724/21

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
			root problem, it is hard to determine when the issue appears. **CVE ID: CVE-2024-3800**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jun-2024	6.1	Sites managed in S@M CMS (Concept Intermedia) might be vulnerable to Reflected XSS via including scripts in one of GET header parameters. Only a part of observed services is vulnerable, but since vendor has not investigated the root problem, it is hard to determine when the issue appears. **CVE ID: CVE-2024-3801**	N/A	A-CON-S\@M-100724/22
Vendor: cozmoslabs					
Product: user_profile_picture					
Affected Version(s): * Up to (excluding) 2.6.2					
Authorization Bypass Through User-Controlled Key	21-Jun-2024	4.3	The User Profile Picture plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.6.1 via the 'rest_api_change_profile_image' function due to missing validation	https://plugins.trac.wordpress.org/changeset/3105132/	A-COZ-USER-100724/23

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on a user controlled key. This makes it possible for authenticated attackers, with Author-level access and above, to update the profile picture of any user. **CVE ID: CVE-2024-5639**		
Vendor: cryoutcreations					
Product: serious_slider					
Affected Version(s): * Up to (excluding) 1.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Cryout Creations Serious Slider allows Stored XSS.This issue affects Serious Slider: from n/a through 1.2.4. **CVE ID: CVE-2024-35762**	N/A	A-CRY-SERI-100724/24
Vendor: darteweb					
Product: dimage_360					
Affected Version(s): * Up to (including) 2.0					
Improper Neutralization of Input During Web Page Generation	21-Jun-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in	N/A	A-DAR-DIMA-100724/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			D'arteweb DImage 360 allows Stored XSS.This issue affects DImage 360: from n/a through 2.0. **CVE ID: CVE-2024-35774**		
Vendor: davekiss					
Product: vimeography					
Affected Version(s): * Up to (excluding) 2.4.2					
Cross-Site Request Forgery (CSRF)	21-Jun-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Dave Kiss Vimeography: Vimeo Video Gallery WordPress Plugin.This issue affects Vimeography: Vimeo Video Gallery WordPress Plugin: from n/a through 2.4.1. **CVE ID: CVE-2024-35770**	N/A	A-DAV-VIME-100724/26
Vendor: detheme					
Product: dethemekit_for_elementor					
Affected Version(s): * Up to (excluding) 2.1.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jun-2024	5.4	The DethemeKit For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the URL parameter of the De Gallery widget in all versions up to and	N/A	A-DET-DETH-100724/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including 2.1.5 due to insufficient input sanitization and output escaping on user-supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user clicks on the injected link. **CVE ID: CVE-2024-6283**		
Vendor: devnath_verma					
Product: widget_bundle					
Affected Version(s): * Up to (including) 2.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-2024	6.1	The Widget Bundle WordPress plugin through 2.0.0 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against only unauthenticated users **CVE ID: CVE-2024-4616**	N/A	A-DEV-WIDG-100724/28
Improper Neutralization of Input During	21-Jun-2024	4.8	The Widget Bundle WordPress plugin through 2.0.0 does not sanitise and	N/A	A-DEV-WIDG-100724/29

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')			escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID: CVE-2024-4970**		
Cross-Site Request Forgery (CSRF)	21-Jun-2024	4.3	The Widget Bundle WordPress plugin through 2.0.0 does not have CSRF checks when logging Widgets, which could allow attackers to make logged in admin enable/disable widgets via a CSRF attack **CVE ID: CVE-2024-4969**	N/A	A-DEV-WIDG-100724/30
Vendor: elegantthemes					
Product: divi					
Affected Version(s): * Up to (excluding) 4.25.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jun-2024	5.4	The Divi theme for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 4.25.1 due to insufficient input sanitization and output	N/A	A-ELE-DIVI-100724/31

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
			escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-5533**		
Vendor: Ericsson					
Product: codechecker					
Affected Version(s): * Up to (excluding) 6.23.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-Jun-2024	6.5	CodeChecker is an analyzer tooling, defect database and viewer extension for the Clang Static Analyzer and Clang Tidy. Zip files uploaded to the server endpoint of `CodeChecker store` are not properly sanitized. An attacker, using a path traversal attack, can load and display files on the machine of `CodeChecker server`. The vulnerable endpoint is `/Default/v6.53/CodeCheckerService@massStoreRun`. The path traversal	https://github.com/Ericsson/codechecker/commit/46bada41e32f3ba0f6011d5c556b579f6dddf07a, https://github.com/Ericsson/codechecker/security/advisories/GHSA-h26w-r4m5-8rrf	A-ERI-CODE-100724/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows reading data on the machine of the `CodeChecker server`, with the same permission level as the `CodeChecker server`. The attack requires a user account on the `CodeChecker server`, with permission to store to a server, and view the stored report. This vulnerability has been patched in version 6.23. **CVE ID: CVE-2023-49793**		
Vendor: erikeng					
Product: google_cse					
Affected Version(s): * Up to (including) 1.0.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-2024	4.8	The Google CSE WordPress plugin through 1.0.7 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	N/A	A-ERI-GOOG-100724/33

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-2024-4755		
Vendor: exeebit					
Product: phpinfo-wp					
Affected Version(s): * Up to (including) 5.0					
N/A	21-Jun-2024	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Exeebit phpinfo() WP.This issue affects phpinfo() WP: from n/a through 5.0. **CVE ID: CVE-2024-35776**	N/A	A-EXE-PHPI-100724/34
Vendor: expert_invoice_project					
Product: expert_invoice					
Affected Version(s): * Up to (including) 1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jun-2024	4.8	The Expert Invoice WordPress plugin through 1.0.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID: CVE-2024-5172**	N/A	A-EXP-EXPE-100724/35
Vendor: finesoft_project					

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: finesoft					
Affected Version(s): * Up to (including) 8.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jun-2024	6.1	Cross Site Scripting vulnerability in Hangzhou Meisoft Information Technology Co., Ltd. Finesoft v.8.0 and before allows a remote attacker to execute arbitrary code via a crafted script to the login.jsp parameter. **CVE ID: CVE-2024-37679**	N/A	A-FIN-FINE-100724/36
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jun-2024	6.1	Hangzhou Meisoft Information Technology Co., Ltd. FineSoft <=8.0 is affected by Cross Site Scripting (XSS) which allows remote attackers to execute arbitrary code. Enter any account and password, click Login, the page will report an error, and a controllable parameter will appear at the URL:weburl. **CVE ID: CVE-2024-37680**	N/A	A-FIN-FINE-100724/37
Vendor: fooplugins					
Product: foobox					
Affected Version(s): * Up to (excluding) 2.7.28					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jun-2024	4.8	The Lightbox & Modal Popup WordPress Plugin WordPress plugin before 2.7.28, foobox-image-lightbox-premium WordPress plugin before 2.7.28 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID: CVE-2024-3276**	N/A	A-FOO-FOOB-100724/38
Vendor: Freedesktop					
Product: poppler					
Affected Version(s): * Up to (excluding) 24.06.0					
N/A	21-Jun-2024	7.5	A flaw was found in the Poppler's Pdfinfo utility. This issue occurs when using -dests parameter with pdfinfo utility. By using certain malformed input files, an attacker could cause the utility to crash, leading to a denial of service.	https://bugzilla.redhat.com/show_bug.cgi?id=2293594	A-FRE-POPP-100724/39

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-2024-6239		
Vendor: fusionplugin					
Product: table_addons_for_elementor					
Affected Version(s): * Up to (excluding) 2.1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jun-2024	5.4	The Table Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '_id' parameter in all versions up to, and including, 2.1.2 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-2024-4313**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3104753%40table-addons-for-elementor&new=3104753%40table-addons-for-elementor&sfp_email=&sfph_mail=#file57	A-FUS-TABL-100724/40
Vendor: Gitlab					
Product: gitlab					
Affected Version(s): 17.1.0					
N/A	27-Jun-2024	8.8	An issue was discovered in GitLab CE/EE affecting all versions starting from 15.8 prior to	N/A	A-GIT-GITL-100724/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows an attacker to trigger a pipeline as another user under certain circumstances. **CVE ID: CVE-2024-5655**		
Incorrect Authorization	27-Jun-2024	7.5	Improper authorization in global search in GitLab EE affecting all versions from 16.11 prior to 16.11.5 and 17.0 prior to 17.0.3 and 17.1 prior to 17.1.1 allows an attacker leak content of a private repository in a public project. **CVE ID: CVE-2024-6323**	N/A	A-GIT-GITL-100724/42
N/A	27-Jun-2024	6.5	An issue was discovered in GitLab CE/EE affecting all versions starting from 9.2 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, with the processing logic for generating link in dependency files can lead to a regular	N/A	A-GIT-GITL-100724/43

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
			expression DoS attack on the server **CVE ID: CVE-2024-1493**		
N/A	27-Jun-2024	6.5	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.7 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows private job artifacts can be accessed by any user. **CVE ID: CVE-2024-3959**	N/A	A-GIT-GITL-100724/44
Uncontrolled Resource Consumption	27-Jun-2024	6.5	Multiple Denial of Service (DoS) conditions has been discovered in GitLab CE/EE affecting all versions starting from 1.0 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1 which allowed an attacker to cause resource exhaustion via banzai pipeline. **CVE ID: CVE-2024-4557**	N/A	A-GIT-GITL-100724/45
N/A	27-Jun-2024	5.5	An issue was discovered in GitLab CE/EE	N/A	A-GIT-GITL-100724/46

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
			affecting all versions starting from 12.0 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows for an attacker to cause a denial of service using a crafted OpenAPI file. **CVE ID: CVE-2024-1816**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jun-2024	5.4	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.9 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, where a stored XSS vulnerability could be imported from a project with malicious commit notes. **CVE ID: CVE-2024-4901**	N/A	A-GIT-GITL-100724/47
N/A	27-Jun-2024	5.3	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.9 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting	N/A	A-GIT-GITL-100724/48

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
			from 17.1 prior to 17.1.1, which allows merge request title to be visible publicly despite being set as project members only. **CVE ID: CVE-2024-2191**		
N/A	27-Jun-2024	4.9	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.10 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows a project maintainer can delete the merge request approval policy via graphQL. **CVE ID: CVE-2024-5430**	N/A	A-GIT-GITL-100724/49
Missing Authorization	27-Jun-2024	4.3	An issue was discovered in GitLab EE affecting all versions starting from 16.0 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows an attacker to access issues and epics without having an SSO	N/A	A-GIT-GITL-100724/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session using Duo Chat. **CVE ID: CVE-2024-3115**		
Incorrect Authorization	27-Jun-2024	4.3	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.1 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows non-project member to promote key results to objectives. **CVE ID: CVE-2024-4011**	N/A	A-GIT-GITL-100724/51
Affected Version(s): From (including) 1.0.0 Up to (excluding) 16.11.5					
Uncontrolled Resource Consumption	27-Jun-2024	6.5	Multiple Denial of Service (DoS) conditions has been discovered in GitLab CE/EE affecting all versions starting from 1.0 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1 which allowed an attacker to cause resource exhaustion via banzai pipeline. **CVE ID: CVE-2024-4557**	N/A	A-GIT-GITL-100724/52

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) 12.0 Up to (excluding) 16.11.5					
N/A	27-Jun-2024	5.5	An issue was discovered in GitLab CE/EE affecting all versions starting from 12.0 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows for an attacker to cause a denial of service using a crafted OpenAPI file. **CVE ID: CVE-2024-1816**	N/A	A-GIT-GITL-100724/53
Affected Version(s): From (including) 15.8.0 Up to (excluding) 16.11.5					
N/A	27-Jun-2024	8.8	An issue was discovered in GitLab CE/EE affecting all versions starting from 15.8 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows an attacker to trigger a pipeline as another user under certain circumstances. **CVE ID: CVE-2024-5655**	N/A	A-GIT-GITL-100724/54
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.11.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	27-Jun-2024	4.3	An issue was discovered in GitLab EE affecting all versions starting from 16.0 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows an attacker to access issues and epics without having an SSO session using Duo Chat. **CVE ID: CVE-2024-3115**	N/A	A-GIT-GITL-100724/55
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.11.5					
Incorrect Authorization	27-Jun-2024	4.3	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.1 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows non-project member to promote key results to objectives. **CVE ID: CVE-2024-4011**	N/A	A-GIT-GITL-100724/56
Affected Version(s): From (including) 16.10.0 Up to (excluding) 16.11.5					
N/A	27-Jun-2024	4.9	An issue was discovered in GitLab CE/EE affecting all versions starting	N/A	A-GIT-GITL-100724/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from 16.10 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows a project maintainer can delete the merge request approval policy via graphQL. **CVE ID: CVE-2024-5430**		
Affected Version(s): From (including) 16.11.0 Up to (excluding) 16.11.5					
Incorrect Authorization	27-Jun-2024	7.5	Improper authorization in global search in GitLab EE affecting all versions from 16.11 prior to 16.11.5 and 17.0 prior to 17.0.3 and 17.1 prior to 17.1.1 allows an attacker leak content of a private repository in a public project. **CVE ID: CVE-2024-6323**	N/A	A-GIT-GITL-100724/58
Affected Version(s): From (including) 16.7.0 Up to (excluding) 16.11.5					
N/A	27-Jun-2024	6.5	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.7 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows private job artifacts	N/A	A-GIT-GITL-100724/59

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
			can be accessed by any user. **CVE ID: CVE-2024-3959**		
Affected Version(s): From (including) 16.9.0 Up to (excluding) 16.11.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jun-2024	5.4	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.9 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, where a stored XSS vulnerability could be imported from a project with malicious commit notes. **CVE ID: CVE-2024-4901**	N/A	A-GIT-GITL-100724/60
N/A	27-Jun-2024	5.3	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.9 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows merge request title to be visible publicly despite being set as project members only. **CVE ID: CVE-2024-2191**	N/A	A-GIT-GITL-100724/61

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) 17.0.0 Up to (excluding) 17.0.3					
N/A	27-Jun-2024	8.8	An issue was discovered in GitLab CE/EE affecting all versions starting from 15.8 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows an attacker to trigger a pipeline as another user under certain circumstances. **CVE ID: CVE-2024-5655**	N/A	A-GIT-GITL-100724/62
Incorrect Authorization	27-Jun-2024	7.5	Improper authorization in global search in GitLab EE affecting all versions from 16.11 prior to 16.11.5 and 17.0 prior to 17.0.3 and 17.1 prior to 17.1.1 allows an attacker leak content of a private repository in a public project. **CVE ID: CVE-2024-6323**	N/A	A-GIT-GITL-100724/63
N/A	27-Jun-2024	6.5	An issue was discovered in GitLab CE/EE affecting all versions starting from 9.2 prior to 16.11.5, starting from 17.0 prior to	N/A	A-GIT-GITL-100724/64

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			17.0.3, and starting from 17.1 prior to 17.1.1, with the processing logic for generating link in dependency files can lead to a regular expression DoS attack on the server **CVE ID: CVE-2024-1493**		
N/A	27-Jun-2024	6.5	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.7 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows private job artifacts can be accessed by any user. **CVE ID: CVE-2024-3959**	N/A	A-GIT-GITL-100724/65
Uncontrolled Resource Consumption	27-Jun-2024	6.5	Multiple Denial of Service (DoS) conditions has been discovered in GitLab CE/EE affecting all versions starting from 1.0 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1 which allowed an attacker to cause resource	N/A	A-GIT-GITL-100724/66

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exhaustion via banzai pipeline. **CVE ID: CVE-2024-4557**		
N/A	27-Jun-2024	5.5	An issue was discovered in GitLab CE/EE affecting all versions starting from 12.0 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows for an attacker to cause a denial of service using a crafted OpenAPI file. **CVE ID: CVE-2024-1816**	N/A	A-GIT-GITL-100724/67
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jun-2024	5.4	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.9 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, where a stored XSS vulnerability could be imported from a project with malicious commit notes. **CVE ID: CVE-2024-4901**	N/A	A-GIT-GITL-100724/68

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-Jun-2024	5.3	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.9 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows merge request title to be visible publicly despite being set as project members only. **CVE ID: CVE-2024-2191**	N/A	A-GIT-GITL-100724/69
N/A	27-Jun-2024	4.9	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.10 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows a project maintainer can delete the merge request approval policy via graphQL. **CVE ID: CVE-2024-5430**	N/A	A-GIT-GITL-100724/70
Missing Authorization	27-Jun-2024	4.3	An issue was discovered in GitLab EE affecting all versions starting from 16.0 prior to 16.11.5, starting from 17.0 prior to	N/A	A-GIT-GITL-100724/71

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
			17.0.3, and starting from 17.1 prior to 17.1.1, which allows an attacker to access issues and epics without having an SSO session using Duo Chat. **CVE ID: CVE-2024-3115**		
Incorrect Authorization	27-Jun-2024	4.3	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.1 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows non-project member to promote key results to objectives. **CVE ID: CVE-2024-4011**	N/A	A-GIT-GITL-100724/72
Affected Version(s): From (including) 9.2.0 Up to (excluding) 16.11.5					
N/A	27-Jun-2024	6.5	An issue was discovered in GitLab CE/EE affecting all versions starting from 9.2 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, with the processing logic for generating link in	N/A	A-GIT-GITL-100724/73

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
			dependency files can lead to a regular expression DoS attack on the server **CVE ID: CVE-2024-1493**		
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 126.0.6478.114					
Access of Resource Using Incompatible Type ('Type Confusion')	20-Jun-2024	8.8	Type Confusion in V8 in Google Chrome prior to 126.0.6478.114 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-6100**	N/A	A-GOO-CHRO-100724/74
N/A	20-Jun-2024	8.8	Inappropriate implementation in V8 in Google Chrome prior to 126.0.6478.114 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-6101**	N/A	A-GOO-CHRO-100724/75
Out-of-bounds Write	20-Jun-2024	8.8	Out of bounds memory access in Dawn in Google Chrome prior to 126.0.6478.114	N/A	A-GOO-CHRO-100724/76

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
			allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-6102**		
Use After Free	20-Jun-2024	8.8	Use after free in Dawn in Google Chrome prior to 126.0.6478.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-6103**	N/A	A-GOO-CHRO-100724/77
Vendor: grey_opaque_project					
Product: grey_opaque					
Affected Version(s): * Up to (including) 2.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jun-2024	5.4	The Grey Opaque theme for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter within the theme's Download-Button shortcode in all versions up to, and including, 2.0.1 due to insufficient input sanitization and output escaping.	N/A	A-GRE-GREY-100724/78

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
			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-2024-5966**		
Vendor: gutenbergforms					
Product: gutenberg_forms					
Affected Version(s): * Up to (excluding) 2.2.9					
Missing Authorization	21-Jun-2024	8.8	Missing Authorization vulnerability in Nikolay Strikhar WordPress Form Builder Plugin – Gutenberg Forms.This issue affects WordPress Form Builder Plugin – Gutenberg Forms: from n/a through 2.2.8.3. **CVE ID: CVE-2022-45803**	N/A	A-GUT-GUTE-100724/79
Vendor: gvectors					
Product: wpforo_forum					
Affected Version(s): * Up to (excluding) 2.1.0					
Improper Neutralization of Input During Web Page	21-Jun-2024	5.4	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic	N/A	A-GVE-WPFO-100724/80

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			XSS) vulnerability in gVectors Team wpForo Forum allows Content Spoofing.This issue affects wpForo Forum: from n/a through 2.0.9. **CVE ID: CVE-2022-38055**		
Vendor: h5p					
Product: h5p					
Affected Version(s): * Up to (excluding) 1.15.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jun-2024	5.4	The Interactive Content WordPress plugin before 1.15.8 does not validate uploads which could allow a Contributors and above to update malicious SVG files, leading to Stored Cross-Site Scripting issues **CVE ID: CVE-2024-3111**	N/A	A-H5P-H5P-100724/81
Vendor: hashicorp					
Product: retryablehttp					
Affected Version(s): * Up to (excluding) 0.7.7					
Insertion of Sensitive Information into Log File	24-Jun-2024	5.5	go-retryablehttp prior to 0.7.7 did not sanitize urls when writing them to its log file. This could lead to go-retryablehttp writing sensitive HTTP basic auth credentials to its log	https://discuss.hashicorp.com/c/security	A-HAS-RETR-100724/82

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
			file. This vulnerability, CVE-2024-6104, was fixed in go-retryablehttp 0.7.7. **CVE ID: CVE-2024-6104**		
Vendor: health_care_hospital_management_system_project					
Product: health_care_hospital_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jun-2024	6.1	CodeProjects Restaurant Reservation System v1.0 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the Date parameter at index.php. **CVE ID: CVE-2024-37800**	N/A	A-HEA-HEAL-100724/83
Vendor: j11g					
Product: cruddiy					
Affected Version(s): * Up to (including) 202312.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jun-2024	7.8	The CRUDDIY project is vulnerable to shell command injection via sending a crafted POST request to the application server. The exploitation risk is limited since CRUDDIY is meant to be launched locally. Nevertheless, a user with the project	N/A	A-J11-CRUD-100724/84

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running on their computer might visit a website which would send such a malicious request to the locally launched server. **CVE ID: CVE-2024-4748**		
Vendor: kadencewp					
Product: gutenberg_blocks_with_ai					
Affected Version(s): * Up to (excluding) 3.2.43					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jun-2024	5.4	The Gutenberg Blocks with AI by Kadence WP – Page Builder Features plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Google Maps widget parameters in all versions up to, and including, 3.2.42 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.	N/A	A-KAD-GUTE-100724/85

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
			CVE ID: CVE-2024-5289		
Product: kadence_blocks_pro					
Affected Version(s): * Up to (excluding) 2.3.8					
N/A	27-Jun-2024	4.3	The kadence-blocks-pro WordPress plugin before 2.3.8 does not prevent users with at least the contributor role using some of its shortcode's functionalities to leak arbitrary options from the database. **CVE ID: CVE-2024-1330**	N/A	A-KAD-KADE-100724/86
Vendor: kubiq					
Product: wp_svg_images					
Affected Version(s): * Up to (excluding) 4.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-2024	5.4	The WP SVG Images plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'type' parameter in all versions up to, and including, 4.2 due to insufficient input sanitization. This makes it possible for authenticated attackers, with Author-level access and above, who have permissions to upload sanitized	https://plugins.trac.wordpress.org/changeset/3105276/	A-KUB-WP_S-100724/87

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files, to bypass SVG sanitization and inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-5945**		
Vendor: LG					
Product: supersign_cms					
Affected Version(s): From (including) 4.1.3 Up to (excluding) 4.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jun-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in LG Electronics SuperSign CMS allows Reflected XSS. This issue affects SuperSign CMS: from 4.1.3 before < 4.3.1. **CVE ID: CVE-2024-6177**	https://lgsecurity.lge.com/bulletins/idproducts#updateDetails	A-LG-SUPE-100724/88
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jun-2024	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LG Electronics SuperSign CMS allows Reflected XSS. This issue affects SuperSign	https://lgsecurity.lge.com/bulletins/idproducts#updateDetails	A-LG-SUPE-100724/89

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
			CMS: from 4.1.3 before < 4.3.1. **CVE ID: CVE-2024-6178**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jun-2024	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LG Electronics SuperSign CMS allows Reflected XSS. This issue affects SuperSign CMS: from 4.1.3 before < 4.3.1. **CVE ID: CVE-2024-6179**	https://lgsecurity.lge.com/bulletins/idproducts#updateDetails	A-LG-SUPE-100724/90
Vendor: livecomposerplugin					
Product: live-composer-page-builder					
Affected Version(s): * Up to (including) 1.5.42					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Live Composer Team Page Builder: Live Composer allows Stored XSS.This issue affects Page Builder: Live Composer: from n/a through 1.5.42. **CVE ID: CVE-2024-35779**	N/A	A-LIV-LIVE-100724/91

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')	21-Jun-2024	4.8	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Live Composer Team Page Builder: Live Composer allows Stored XSS.This issue affects Page Builder: Live Composer: from n/a through 1.5.42. **CVE ID: CVE-2024-35768**	N/A	A-LIV-LIVE-100724/92
Vendor: mediavine					
Product: create					
Affected Version(s): * Up to (excluding) 1.9.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jun-2024	5.4	The Create by Mediavine plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Schema Meta shortcode in all versions up to, and including, 1.9.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that	https://plugins.trac.wordpress.org/changeset/3108144/#file794	A-MED-CREA-100724/93

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-5601**		
Vendor: melapress					
Product: wp_2fa					
Affected Version(s): * Up to (excluding) 2.6.4					
Insertion of Sensitive Information into Log File	21-Jun-2024	7.5	Insertion of Sensitive Information into Log File vulnerability in WP 2FA allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects WP 2FA: from n/a through 2.6.3. **CVE ID: CVE-2022-44587**	N/A	A-MEL-WP_2-100724/94
Vendor: Microsoft					
Product: sharepoint_server					
Affected Version(s): 2019					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-Jun-2024	9.8	An issue was discovered in VirtoSoftware Virto Bulk File Download 5.5.44 for SharePoint 2019. The Virto.SharePoint.FileDownloader/Api/Download.ashx isCompleted method allows	N/A	A-MIC-SHAR-100724/95

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary file download and deletion via absolute path traversal in the path parameter. **CVE ID: CVE-2024-33879**		
N/A	24-Jun-2024	5.3	An issue was discovered in VirtoSoftware Virto Bulk File Download 5.5.44 for SharePoint 2019. It discloses full pathnames via Virto.SharePoint.FileDownloader/Api/Download.ashx?action=archive. **CVE ID: CVE-2024-33880**	N/A	A-MIC-SHAR-100724/96
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-Jun-2024	5.3	An issue was discovered in VirtoSoftware Virto Bulk File Download 5.5.44 for SharePoint 2019. The Virto.SharePoint.FileDownloader/Api/Download.ashx isCompleted method allows an NTLMv2 hash leak via a UNC share pathname in the path parameter. **CVE ID: CVE-2024-33881**	N/A	A-MIC-SHAR-100724/97
Vendor: mohsinrasool					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: paypal_pay_now\,_buy_now\,_donation_and_cart_buttons_shortcode					
Affected Version(s): * Up to (including) 1.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-2024	5.4	The PayPal Pay Now, Buy Now, Donation and Cart Buttons Shortcode WordPress plugin through 1.7 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID: CVE-2024-5448**	N/A	A-MOH-PAYP-100724/98
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-2024	4.8	The PayPal Pay Now, Buy Now, Donation and Cart Buttons Shortcode WordPress plugin through 1.7 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for	N/A	A-MOH-PAYP-100724/99

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			example in multisite setup) **CVE ID: CVE-2024-5447**		
Vendor: ninjateam					
Product: wp_chat_app					
Affected Version(s): * Up to (excluding) 3.6.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jun-2024	4.8	The WP Chat App WordPress plugin before 3.6.5 does not sanitise and escape some of its settings, which could allow high privilege users such as admins to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed. **CVE ID: CVE-2024-4664**	N/A	A-NIN-WP_C-100724/100
Vendor: onetarek					
Product: wp_logs_book					
Affected Version(s): * Up to (including) 1.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-2024	5.4	The WP Logs Book WordPress plugin through 1.0.1 does not sanitise and escape some of its log data before outputting them back in an admin dashboard, leading to an Unauthenticated Stored Cross-Site Scripting	N/A	A-ONE-WP_L-100724/101

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
			CVE ID: CVE-2024-4477		
Vendor: Opencart					
Product: opencart					
Affected Version(s): 3.0.3.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Jun-2024	8.1	This affects versions of the package opencart/opencart from 0.0.0. An SQL Injection issue was identified in the Divido payment extension for OpenCart, which is included by default in version 3.0.3.9. As an anonymous unauthenticated user, if the Divido payment module is installed (it does not have to be enabled), it is possible to exploit SQL injection to gain unauthorised access to the backend database. For any site which is vulnerable, any unauthenticated user could exploit this to dump the entire OpenCart database, including customer PII data. **CVE ID: CVE-2024-21514**	https://github.com/opencart/opencart/commit/46bd5f5a8056ff9aad0aa7d71729c4cf593d67e2, https://security.snyk.io/vuln/SNYK-PHP-OPENCARTOPENCART-7266565	A-OPE-OPEN-100724/102
Vendor: Parallels					
Product: parallels_desktop					

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) 19.3.0					
Improper Privilege Management	21-Jun-2024	10	Improper privilege management vulnerability in Parallels Desktop Software, which affects versions earlier than 19.3.0. An attacker could add malicious code in a script and populate the BASH_ENV environment variable with the path to the malicious script, executing on application startup. An attacker could exploit this vulnerability to escalate privileges on the system. **CVE ID: CVE-2024-6240**	N/A	A-PAR-PARA-100724/103
Vendor: pearadmin					
Product: pear_admin_boot					
Affected Version(s): * Up to (including) 2.0.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Jun-2024	9.8	A vulnerability was found in Pear Admin Boot up to 2.0.2 and classified as critical. This issue affects the function getDictItems of the file /system/dictData/getDictItems/. The manipulation with the input ,user(),1,1	N/A	A-PEA-PEAR-100724/104

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
			leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-269375. **CVE ID: CVE-2024-6241**		
Vendor: presscustomizr					
Product: customizr					
Affected Version(s): * Up to (excluding) 4.4.22					
Cross-Site Request Forgery (CSRF)	21-Jun-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in presscustomizr Customizr.This issue affects Customizr: from n/a through 4.4.21. **CVE ID: CVE-2024-35771**	N/A	A-PRE-CUST-100724/105
Product: hueman					
Affected Version(s): * Up to (excluding) 3.7.25					
Cross-Site Request Forgery (CSRF)	21-Jun-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in presscustomizr Hueman.This issue affects Hueman: from n/a through 3.7.24. **CVE ID: CVE-2024-35772**	N/A	A-PRE-HUEM-100724/106
Vendor: rarathemes					

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: book_landing_page					
Affected Version(s): * Up to (excluding) 1.2.4					
Cross-Site Request Forgery (CSRF)	21-Jun-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Rara Theme Book Landing Page.This issue affects Book Landing Page: from n/a through 1.2.3. **CVE ID: CVE-2024-37230**	N/A	A-RAR-BOOK-100724/107
Vendor: redlettuce					
Product: pdf_viewer_for_elementor					
Affected Version(s): * Up to (including) 2.9.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jun-2024	5.4	The PDF Viewer for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the render function in all versions up to, and including, 2.9.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-0845**	N/A	A-RED-PDF_-100724/108

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: renesas					
Product: rcar_gen3					
Affected Version(s): v2.5					
Incorrect Calculation	24-Jun-2024	7.8	Incorrect Calculation vulnerability in Renesas arm-trusted-firmware allows Local Execution of Code. When checking whether a new image invades/overlaps with a previously loaded image the code neglects to consider a few cases. that could An attacker to bypass memory range restriction and overwrite an already loaded image partly or completely, which could result in code execution and bypass of secure boot. **CVE ID: CVE-2024-6287**	https://github.com/renesas-rcar/arm-trusted-firmware/commit/954d488a9798f8fda675c6b57c571b469b298f04	A-REN-RCAR-100724/109
Integer Underflow (Wrap or Wraparound)	24-Jun-2024	6.7	Integer Underflow (Wrap or Wraparound) vulnerability in Renesas arm-trusted-firmware.	https://github.com/renesas-rcar/arm-trusted-firmware/commit/b596f580637bae919b0ac	A-REN-RCAR-100724/110

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
			An integer underflow in image range check calculations could lead to bypassing address restrictions and loading of images to unallowed addresses. **CVE ID: CVE-2024-6285**	3a5471422a1f756db3b	
Vendor: Rocklobster					
Product: contact_form_7					
Affected Version(s): * Up to (excluding) 5.9.5					
URL Redirection to Untrusted Site ('Open Redirect')	27-Jun-2024	6.1	The Contact Form 7 WordPress plugin before 5.9.5 has an open redirect that allows an attacker to utilize a false URL and redirect to the URL of their choosing. **CVE ID: CVE-2024-4704**	N/A	A-ROC-CONT-100724/111
Vendor: Sharethis					
Product: simple_share_buttons_adder					
Affected Version(s): * Up to (excluding) 8.5.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jun-2024	5.4	The Simple Share Buttons Adder WordPress plugin before 8.5.1 does not sanitise and escape some of its settings, which could allow high privilege users such as editors to perform Cross-Site	N/A	A-SHA-SIMP-100724/112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Scripting attacks even when unfiltered_html is disallowed **CVE ID: CVE-2024-4094**		
Vendor: slideshow_se_project					
Product: slideshow_se					
Affected Version(s): * Up to (including) 2.5.17					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Jun-2024	8.8	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in John West Slideshow SE allows PHP Local File Inclusion.This issue affects Slideshow SE: from n/a through 2.5.17. **CVE ID: CVE-2024-35778**	N/A	A-SLI-SLID-100724/113
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-2024	4.8	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in John West Slideshow SE allows Stored XSS.This issue affects Slideshow SE: from n/a through 2.5.17. **CVE ID: CVE-2024-35769**	N/A	A-SLI-SLID-100724/114
Vendor: solidwp					

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: solid_security					
Affected Version(s): * Up to (excluding) 9.3.2					
Insufficient Verification of Data Authenticity	21-Jun-2024	5.3	Use of Less Trusted Source vulnerability in SolidWP Solid Security allows HTTP DoS.This issue affects Solid Security: from n/a through 9.3.1. **CVE ID: CVE-2022-44593**	N/A	A-SOL-SOLI-100724/115
Vendor: squeeze_project					
Product: squeeze					
Affected Version(s): * Up to (excluding) 1.4.1					
Unrestricted Upload of File with Dangerous Type	21-Jun-2024	7.2	Unrestricted Upload of File with Dangerous Type vulnerability in Bogdan Bendziukov Squeeze allows Code Injection.This issue affects Squeeze: from n/a through 1.4. **CVE ID: CVE-2024-35767**	N/A	A-SQU-SQUE-100724/116
Vendor: startbooking					
Product: scheduling_plugin_-_online_booking					
Affected Version(s): * Up to (including) 3.5.10					
Missing Authorization	18-Jun-2024	6.5	The Scheduling Plugin – Online Booking for WordPress plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability	N/A	A-STA-SCHE-100724/117

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
			check on the 'cbsb_disconnect_settings' function in all versions up to, and including, 3.5.10. This makes it possible for unauthenticated attackers to disconnect the plugin from the startbooking service and remove connection data. **CVE ID: CVE-2024-1634**		
Vendor: tessi					
Product: docubase					
Affected Version(s): 5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-2024	5.4	Cross Site Scripting vulnerability in Tessi Docubase Document Management product 5.x allows a remote attacker to execute arbitrary code via the page parameter. **CVE ID: CVE-2024-37671**	N/A	A-TES-DOCU-100724/118
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-2024	5.4	Cross Site Scripting vulnerability in Tessi Docubase Document Management product 5.x allows a remote attacker to execute arbitrary code via the	N/A	A-TES-DOCU-100724/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			idactivity parameter. **CVE ID: CVE-2024-37672**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-2024	5.4	Cross Site Scripting vulnerability in Tessi Docubase Document Management product 5.x allows a remote attacker to execute arbitrary code via the filename parameter. **CVE ID: CVE-2024-37673**	N/A	A-TES-DOCU-100724/120
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-2024	5.4	Cross Site Scripting vulnerability in Tessi Docubase Document Management product 5.x allows a remote attacker to execute arbitrary code via the parameter "sectionContent" related to the functionality of adding notes to an uploaded file. **CVE ID: CVE-2024-37675**	N/A	A-TES-DOCU-100724/121
Vendor: themefreesia					
Product: excellent					
Affected Version(s): * Up to (excluding) 1.3.0					
Improper Neutralization of Input During	21-Jun-2024	5.4	Improper Neutralization of Input During Web Page Generation	N/A	A-THE-EXCE-100724/122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			(XSS or 'Cross-site Scripting') vulnerability in Theme Freesia Excellent allows Stored XSS.This issue affects Excellent: from n/a through 1.2.9. **CVE ID: CVE-2024-35763**		
Vendor: themehorse					
Product: interface					
Affected Version(s): * Up to (excluding) 3.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Theme Horse Interface allows Stored XSS.This issue affects Interface: from n/a through 3.1.0. **CVE ID: CVE-2024-35758**	N/A	A-THE-INTE-100724/123
Vendor: themeisle					
Product: orbit_fox					
Affected Version(s): * Up to (excluding) 2.10.35					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jun-2024	5.4	The Orbit Fox by ThemeIsle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Services and Post Type Grid widgets	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3055876%40themeisle-	A-THE-ORBI-100724/124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in all versions up to, and including, 2.10.34 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-2024-2484**	companion&new=3055876%40themeisle-companion&sfp_email=&sfph_mail=	
Vendor: themify					
Product: product_filter					
Affected Version(s): * Up to (excluding) 1.5.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Jun-2024	7.5	The Themify – WooCommerce Product Filter plugin for WordPress is vulnerable to time-based SQL Injection via the 'conditions' parameter in all versions up to, and including, 1.4.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it	N/A	A-THE-PROD-100724/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2024-6027**		
Vendor: tickera					
Product: tickera					
Affected Version(s): * Up to (excluding) 3.5.2.9					
Incorrect Authorization	18-Jun-2024	4.3	The Tickera – WordPress Event Ticketing plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the tc_dl_delete_tickets AJAX action in all versions up to, and including, 3.5.2.8. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete all tickets associated with events. **CVE ID: CVE-2024-5860**	N/A	A-TIC-TICK-100724/126
Vendor: tms-outsource					
Product: amelia					

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) 1.1.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-2024	4.8	The Booking for Appointments and Events Calendar – Amelia plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.1.5 (and 7.5.1 for the Pro version) due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID: CVE-2024-6225**	N/A	A-TMS-AMEL-100724/127
Vendor: Tribulant					
Product: newsletters					
Affected Version(s): * Up to (excluding) 4.9.8					
Cross-Site Request	21-Jun-2024	8.8	Cross Site Request Forgery (CSRF)	N/A	A-TRI-NEWS-100724/128

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
Forgery (CSRF)			vulnerability in Tribulant Newsletters.This issue affects Newsletters: from n/a through 4.9.7. **CVE ID: CVE-2024-37227**		
Vendor: trudesk_project					
Product: trudesk					
Affected Version(s): 1.1.11					
Cross-Site Request Forgery (CSRF)	24-Jun-2024	6.5	TruDesk Help Desk/Ticketing Solution v1.1.11 is vulnerable to a Cross-Site Request Forgery (CSRF) attack which would allow an attacker to restart the server, causing a DoS attack. The attacker must craft a webpage that would perform a GET request to the /api/v1/admin/restart endpoint, then the victim (who has sufficient privileges), would visit the page and the server restart would begin. The attacker must know the full URL that TruDesk is on in order to craft the webpage. **CVE ID: CVE-2021-45785**	N/A	A-TRU-TRUD-100724/129

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: tvsmotor					
Product: tvs_connect					
Affected Version(s): 4.6.0					
Use of a Broken or Risky Cryptographic Algorithm	21-Jun-2024	7.5	TVS Motor Company Limited TVS Connect Android v4.6.0 and IOS v5.0.0 was discovered to insecurely handle the RSA key pair, allowing attackers to possibly access sensitive information via decryption. **CVE ID: CVE-2024-35537**	N/A	A-TVS-TVS_-100724/130
Affected Version(s): 5.0.0					
Use of a Broken or Risky Cryptographic Algorithm	21-Jun-2024	7.5	TVS Motor Company Limited TVS Connect Android v4.6.0 and IOS v5.0.0 was discovered to insecurely handle the RSA key pair, allowing attackers to possibly access sensitive information via decryption. **CVE ID: CVE-2024-35537**	N/A	A-TVS-TVS_-100724/131
Vendor: uncannyowl					
Product: uncanny_automator					
Affected Version(s): * Up to (including) 5.3					
Cross-Site Request	21-Jun-2024	8.8	Cross Site Request Forgery (CSRF) vulnerability in	N/A	A-UNC-UNCA-100724/132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			Uncanny Owl Uncanny Automator Pro.This issue affects Uncanny Automator Pro: from n/a through 5.3. **CVE ID: CVE-2024-37118**		
Vendor: unknown-corp					
Product: melty_blood_actress_again_current_code					
Affected Version(s): * Up to (including) 1.07					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	28-Jun-2024	9.8	Soft Circle French-Bread Melty Blood: Actress Again: Current Code through 1.07 Rev. 1.4.0 allows a remote attacker to execute arbitrary code on a client's machine via a crafted packet on TCP port 46318. **CVE ID: CVE-2024-39704**	N/A	A-UNK-MELT-100724/133
Vendor: uxthemes					
Product: flatsome					
Affected Version(s): * Up to (excluding) 3.19.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jun-2024	5.4	The Flatsome theme for WordPress is vulnerable to Stored Cross-Site Scripting via the UX Countdown, Video Button, UX Video, UX Slider, UX Sidebar, and UX	N/A	A-UXT-FLAT-100724/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Payment Icons shortcodes in all versions up to, and including, 3.18.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-5346**		
Vendor: vcita					
Product: online_booking_\&_scheduling_calendar_for_wordpress_by_vcita					
Affected Version(s): * Up to (excluding) 4.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-2024	6.1	The Online Booking & Scheduling Calendar for WordPress by vcita plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'd' parameter in all versions up to, and including, 4.4.2 due to insufficient input sanitization and output escaping. This makes it possible for	N/A	A-VCI-ONLI-100724/135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2024-5859**		
Affected Version(s): * Up to (excluding) 4.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in vCita Online Booking & Scheduling Calendar for WordPress by vcita allows Stored XSS.This issue affects Online Booking & Scheduling Calendar for WordPress by vcita: from n/a through 4.4.0. **CVE ID: CVE-2024-35761**	N/A	A-VCI-ONLI-100724/136
Affected Version(s): * Up to (excluding) 4.4.3					
Improper Neutralization of Input During Web Page	22-Jun-2024	6.1	The Online Booking & Scheduling Calendar for WordPress by vcita plugin for	N/A	A-VCI-ONLI-100724/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			WordPress is vulnerable to Stored Cross-Site Scripting via the 'wp_id' parameter in all versions up to, and including, 4.4.2 due to missing authorization checks on processAction function, as well as insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that will execute whenever a user accesses a wp-admin dashboard. **CVE ID: CVE-2024-5791**		
Vendor: virtosoftware					
Product: sharepoint_bulk_file_download					
Affected Version(s): 5.5.44					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-Jun-2024	9.8	An issue was discovered in VirtoSoftware Virto Bulk File Download 5.5.44 for SharePoint 2019. The Virto.SharePoint.FileDownloader/Api/Download.ashx isCompleted method allows arbitrary file	N/A	A-VIR-SHAR-100724/138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			download and deletion via absolute path traversal in the path parameter. **CVE ID: CVE-2024-33879**		
N/A	24-Jun-2024	5.3	An issue was discovered in VirtoSoftware Virto Bulk File Download 5.5.44 for SharePoint 2019. It discloses full pathnames via Virto.SharePoint.FileDownloader/Api/Download.ashx?action=archive. **CVE ID: CVE-2024-33880**	N/A	A-VIR-SHAR-100724/139
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-Jun-2024	5.3	An issue was discovered in VirtoSoftware Virto Bulk File Download 5.5.44 for SharePoint 2019. The Virto.SharePoint.FileDownloader/Api/Download.ashx isCompleted method allows an NTLMv2 hash leak via a UNC share pathname in the path parameter. **CVE ID: CVE-2024-33881**	N/A	A-VIR-SHAR-100724/140
Vendor: vowelweb					
Product: ibtana					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.2.3.3					
N/A	18-Jun-2024	5.3	The Ibtana – WordPress Website Builder plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ibtana_visual_editor_register_ajax_json_endpont' function in all versions up to, and including, 1.2.3.3. This makes it possible for unauthenticated attackers to update option values for reCAPTCHA keys on the WordPress site. This can be leveraged to bypass reCAPTCHA on the site. **CVE ID: CVE-2024-5541**	N/A	A-VOW-IBTA-100724/141
Vendor: webtechstreet					
Product: elementor_addon_elements					
Affected Version(s): * Up to (excluding) 1.13.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jun-2024	5.4	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter in versions up to, and including, 1.13.5	https://plugins.trac.wordpress.org/changeset/3107074/	A-WEB-ELEM-100724/142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-4569**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jun-2024	5.4	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter in versions up to, and including, 1.13.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user	https://plugins.trac.wordpress.org/changeset/3107074/	A-WEB-ELEM-100724/143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accesses an injected page. **CVE ID: CVE-2024-4570**		
Vendor: wildweblab					
Product: mosaic					
Affected Version(s): * Up to (including) 1.7.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jun-2024	5.4	The Mosaic theme for WordPress is vulnerable to Stored Cross-Site Scripting via the 'link' parameter within the theme's Button shortcode in all versions up to, and including, 1.7.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-5965**	N/A	A-WIL-MOSA-100724/144
Vendor: wp-pizza					
Product: wppizza					
Affected Version(s): * Up to (excluding) 3.18.14					
Improper Neutralization of Input	21-Jun-2024	6.1	Improper Neutralization of Input During Web	N/A	A-WP--WPPI-100724/145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Page Generation (XSS or 'Cross-site Scripting') vulnerability in ollybach WPPizza allows Reflected XSS.This issue affects WPPizza: from n/a through 3.18.13. **CVE ID: CVE-2024-35766**		
Vendor: wpdeveloper					
Product: embedpress					
Affected Version(s): * Up to (excluding) 3.8.4					
Missing Authorization	21-Jun-2024	8.8	Missing Authorization vulnerability in WPDeveloper EmbedPress.This issue affects EmbedPress: from n/a through 3.8.3. **CVE ID: CVE-2023-51375**	N/A	A-WPD-EMBE-100724/146
Product: typing_text					
Affected Version(s): * Up to (excluding) 1.2.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPDeveloper Typing Text allows Stored XSS.This issue affects Typing Text: from n/a through 1.2.5.	N/A	A-WPD-TYPI-100724/147

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
			CVE ID: CVE-2024-5058		
Vendor: wpjobportal					
Product: wp_job_portal					
Affected Version(s): * Up to (excluding) 2.1.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-2024	4.8	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Job Portal allows Stored XSS.This issue affects WP Job Portal: from n/a through 2.1.3. **CVE ID: CVE-2024-35759**	N/A	A-WPJ-WP_J-100724/148
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-2024	4.8	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Job Portal allows Stored XSS.This issue affects WP Job Portal: from n/a through 2.1.3. **CVE ID: CVE-2024-35760**	N/A	A-WPJ-WP_J-100724/149
Vendor: wpmudev					
Product: branda					
Affected Version(s): * Up to (excluding) 3.4.18					
Improper Neutralization of Input During	21-Jun-2024	5.4	The Branda – White Label WordPress, Custom Login Page Customizer plugin	https://plugins.trac.wordpress.org/changeset/3104910/	A-WPM-BRAN-100724/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			for WordPress is vulnerable to Stored Cross-Site Scripting via the 'mime_types' parameter in all versions up to, and including, 3.4.17 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-5191**		
Vendor: wpneuron					
Product: sparkle_demo_importer					
Affected Version(s): * Up to (excluding) 1.4.8					
Missing Authorization	22-Jun-2024	6.5	The Sparkle Demo Importer plugin for WordPress is vulnerable to unauthorized database reset and demo data import due to a missing capability check on the multiple functions in all versions up to and including 1.4.7. This makes it possible	N/A	A-WPN-SPAR-100724/151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for authenticated attackers, with Subscriber-level access and above, to delete all posts, pages, and uploaded files, as well as download and install a limited set of demo plugins. **CVE ID: CVE-2024-6120**		
Vendor: Xwiki					
Product: Xwiki					
Affected Version(s): From (including) 1.5 Up to (excluding) 15.0					
Incorrect Authorization	24-Jun-2024	4.3	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The content of a document included using `{{include reference="targetdocument"/}}` is executed with the right of the includer and not with the right of its author. This means that any user able to modify the target document can impersonate the author of the content which used the `include` macro. This vulnerability has been patched in XWiki 15.0 RC1 by	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-qcj3-wpgm-qpxh	A-XWI-XWIK-100724/152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			making the default behavior safe. **CVE ID: CVE-2024-38369**		
Hardware					
Vendor: hanwhavision					
Product: ane-l6012r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-ANE--100724/153
Product: ane-l7012r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated	https://www.hanwhavision.com/wp-content/uploads/2024/06/Ca	H-HAN-ANE--100724/154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	mera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: ano-l6012r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-ANO--100724/155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: ano-l6022r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-ANO--100724/156
Product: ano-l6082r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-ANO--100724/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: ano-l7012r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-ANO--100724/158
Product: ano-l7022r					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-ANO--100724/159
Product: ano-l7082r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-ANO--100724/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: anv-l6012r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-ANV--100724/161
Product: anv-l6023r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-ANV--100724/162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: anv-l6082r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-ANV--100724/163

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
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: anv-l7012r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-ANV--100724/164
Product: anv-l7082r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-ANV--100724/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: lnd-6012r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-LND--100724/166
Product: lnd-6022r					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-LND--100724/167
Product: lnd-6032r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-LND--100724/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: lnd-6072r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-LND--100724/169
Product: lno-6012r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-LNO--100724/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: lno-6022r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-LNO--100724/171

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
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: lno-6032r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-LNO--100724/172
Product: lno-6072r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-LNO--100724/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: lnv-6012r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-LNV--100724/174
Product: lnv-6022r					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-LNV--100724/175
Product: lnv-6032r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-LNV--100724/176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: lnv-6072r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-LNV--100724/177
Product: pnm-12082rvd					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-PNM--100724/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: pnm-7002vd					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-PNM--100724/179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: pnm-7082rvd					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-PNM--100724/180
Product: pnm-8082vt					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-PNM--100724/181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: pnm-9000qb					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-PNM--100724/182
Product: pnm-9002vq					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-PNM--100724/183
Product: pnm-9022v					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-PNM--100724/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: pnm-9031rv					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-PNM--100724/185
Product: pnm-9084qz					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-PNM--100724/186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: pnm-9084qz1					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-PNM--100724/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: pnm-9084rqz					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-PNM--100724/188
Product: pnm-9084rqz1					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-PNM--100724/189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: pnm-9085rqz					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-PNM--100724/190
Product: pnm-9085rqz1					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-PNM--100724/191
Product: pnm-9322vqp					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-PNM--100724/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: pnm-c9022rv					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-PNM--100724/193
Product: qnb-8002					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-QNB--100724/194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: qnd-6011					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QND--100724/195

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
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnd-6012r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QND--100724/196
Product: qnd-6012r1					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-QND--100724/197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: qnd-6021					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QND--100724/198
Product: qnd-6022r					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QND--100724/199
Product: qnd-6022r1					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QND--100724/200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnd-6032r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QND--100724/201
Product: qnd-6032r1					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-QND--100724/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: qnd-6072r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QND--100724/203

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
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnd-6072r1					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QND--100724/204
Product: qnd-6073r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-QND--100724/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: qnd-6082r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QND--100724/206
Product: qnd-6082r1					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QND--100724/207
Product: qnd-6083r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QND--100724/208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnd-7012r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QND--100724/209
Product: qnd-7022r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-QND--100724/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: qnd-7032r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QND--100724/211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnd-7082r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QND--100724/212
Product: qnd-8010r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-QND--100724/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: qnd-8011					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QND--100724/214
Product: qnd-8020r					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QND--100724/215
Product: qnd-8021					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QND--100724/216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnd-8030r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QND--100724/217
Product: qnd-8080r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-QND--100724/218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: qne-8011r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNE--100724/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qne-8021r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNE--100724/220
Product: qno-6012r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-QNO--100724/221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: qno-6012r1					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNO--100724/222
Product: qno-6014r					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNO--100724/223
Product: qno-6022r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNO--100724/224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qno-6022r1					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNO--100724/225
Product: qno-6032r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-QNO--100724/226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: qno-6032r1					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNO--100724/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qno-6072r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNO--100724/228
Product: qno-6072r1					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-QNO--100724/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: qno-6073r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNO--100724/230
Product: qno-6082r					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNO--100724/231
Product: qno-6082r1					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNO--100724/232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qno-6083r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNO--100724/233
Product: qno-6084r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-QNO--100724/234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: qno-7012r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNO--100724/235

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
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qno-7022r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNO--100724/236
Product: qno-7032r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-QNO--100724/237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: qno-7082r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNO--100724/238
Product: qno-8010r					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNO--100724/239
Product: qno-8020r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNO--100724/240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qno-8030r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNO--100724/241
Product: qno-8080r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-QNO--100724/242

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 DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: qnv-6012r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNV--100724/243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnv-6012r1					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNV--100724/244
Product: qnv-6014r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-QNV--100724/245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: qnv-6022r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNV--100724/246
Product: qnv-6022r1					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNV--100724/247
Product: qnv-6023r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNV--100724/248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnv-6024rm					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNV--100724/249
Product: qnv-6032r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-QNV--100724/250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: qnv-6032r1					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNV--100724/251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnv-6072r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNV--100724/252
Product: qnv-6072r1					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-QNV--100724/253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: qnv-6073r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNV--100724/254
Product: qnv-6082r					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNV--100724/255
Product: qnv-6082r1					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNV--100724/256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnv-6083r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNV--100724/257
Product: qnv-6084r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-QNV--100724/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: qnv-7012r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNV--100724/259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnv-7022r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNV--100724/260
Product: qnv-7032r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-QNV--100724/261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: qnv-7082r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNV--100724/262
Product: qnv-8010r					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNV--100724/263
Product: qnv-8020r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNV--100724/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnv-8030r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-QNV--100724/265
Product: qnv-8080r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-QNV--100724/266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: tnv-c7013rc					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-TNV--100724/267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnb-6002					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNB--100724/268
Product: xnb-6003					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-XNB--100724/269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: xnb-8002					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNB--100724/270
Product: xnb-8003					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNB--100724/271
Product: xnb-9002					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNB--100724/272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnb-9003					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNB--100724/273
Product: xnd-6083rv					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-XND--100724/274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: xnd-8082rf					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XND--100724/275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnd-8082rv					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XND--100724/276
Product: xnd-8083rv					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-XND--100724/277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: xnd-8093rv					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XND--100724/278
Product: xnd-9082rf					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XND--100724/279
Product: xnd-9082rv					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XND--100724/280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnd-9083rv					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XND--100724/281
Product: xnd-c6083rv					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-XND--100724/282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: xnd-c7083rv					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XND--100724/283

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
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnd-c8083rv					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XND--100724/284
Product: xnd-c9083rv					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-XND--100724/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: xnf-9010rs					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNF--100724/286
Product: xnf-9010rv					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNF--100724/287
Product: xnf-9010rvm					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNF--100724/288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnf-9013rv					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNF--100724/289
Product: xno-6083r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-XNO--100724/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: xno-6123r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNO--100724/291

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
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xno-8082r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNO--100724/292
Product: xno-8083r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-XNO--100724/293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: xno-9082r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNO--100724/294
Product: xno-9083r					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNO--100724/295
Product: xno-c6083r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNO--100724/296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xno-c7083r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNO--100724/297
Product: xno-c8083r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-XNO--100724/298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: xno-c9083r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNO--100724/299

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
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnp-6400					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNP--100724/300
Product: xnp-6400r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-XNP--100724/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: xnp-6400rw					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNP--100724/302
Product: xnp-8250					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNP--100724/303
Product: xnp-8250r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNP--100724/304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnp-8300rw					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNP--100724/305
Product: xnp-9250					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-XNP--100724/306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: xnp-9250r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNP--100724/307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnp-9300rw					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNP--100724/308
Product: xnp-c6403					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-XNP--100724/309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: xnp-c6403r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNP--100724/310
Product: xnp-c6403rw					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNP--100724/311
Product: xnp-c8253					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNP--100724/312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnp-c8253r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNP--100724/313
Product: xnp-c8303rw					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-XNP--100724/314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: xnp-c9253					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNP--100724/315

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
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnp-c9253r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNP--100724/316
Product: xnp-c9303rw					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-XNP--100724/317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: xnp-c9310r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNP--100724/318
Product: xnv-6083r					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNV--100724/319
Product: xnv-6083rz					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNV--100724/320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnv-6083z					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNV--100724/321
Product: xnv-6123r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-XNV--100724/322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: xnv-8082r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNV--100724/323

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
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnv-8083r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNV--100724/324
Product: xnv-8083rz					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-XNV--100724/325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: xnv-8083z					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNV--100724/326
Product: xnv-8093r					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNV--100724/327
Product: xnv-9082r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNV--100724/328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnv-9083r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNV--100724/329
Product: xnv-9083rz					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a	https://www.hanwhavision.com/wp-content/upload	H-HAN-XNV--100724/330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	s/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: xnv-c6083					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNV--100724/331

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
			report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnv-c6083r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNV--100724/332
Product: xnv-c7083r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-	H-HAN-XNV--100724/333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	2023-5037-5038.pdf	
Product: xnv-c8083r					
Affected Version(s): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNV--100724/334
Product: xnv-c9083r					

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): -					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	H-HAN-XNV--100724/335
Vendor: Omron					
Product: nj-pa3001					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration.	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ-P-100724/336

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-2024-33687		
Product: nj-pd3001					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ-P-100724/337
Product: nj101-1000					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ10-100724/338
Product: nj101-1020					
Affected Version(s): -					

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
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ10-100724/339
Product: nj101-9000					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ10-100724/340
Product: nj101-9020					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all	https://www.fa.omron.co.jp/product/security/assets/pdf/en/	H-OMR-NJ10-100724/341

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
			versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	OMSR-2024-004_en.pdf	
Product: nj301-1100					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ30-100724/342
Product: nj301-1200					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ30-100724/343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**		
Product: nj501-1300					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ50-100724/344
Product: nj501-1320					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration.	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ50-100724/345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33687		
Product: nj501-1340					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ50-100724/346
Product: nj501-140					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ50-100724/347
Product: nj501-1400					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ50-100724/348
Product: nj501-1420					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ50-100724/349
Product: nj501-1500					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all	https://www.fa.omron.co.jp/product/security/assets/pdf/en/	H-OMR-NJ50-100724/350

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
			versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	OMSR-2024-004_en.pdf	
Product: nj501-1520					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ50-100724/351
Product: nj501-4300					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ50-100724/352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**		
Product: nj501-4310					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ50-100724/353
Product: nj501-4320					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration.	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ50-100724/354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33687		
Product: nj501-4400					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ50-100724/355
Product: nj501-4500					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ50-100724/356
Product: nj501-5300					
Affected Version(s): -					

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
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ50-100724/357
Product: nj501-5300-1					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ50-100724/358
Product: nj501-r300					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all	https://www.fa.omron.co.jp/product/security/assets/pdf/en/	H-OMR-NJ50-100724/359

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
			versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	OMSR-2024-004_en.pdf	
Product: nj501-r320					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ50-100724/360
Product: nj501-r400					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ50-100724/361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**		
Product: nj501-r420					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ50-100724/362
Product: nj501-r500					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration.	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ50-100724/363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33687		
Product: nj501-r520					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NJ50-100724/364
Product: nx102-1000					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX10-100724/365
Product: nx102-1020					
Affected Version(s): -					

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
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX10-100724/366
Product: nx102-1100					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX10-100724/367
Product: nx102-1120					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all	https://www.fa.omron.co.jp/product/security/assets/pdf/en/	H-OMR-NX10-100724/368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	OMSR-2024-004_en.pdf	
Product: nx102-1200					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX10-100724/369
Product: nx102-1220					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX10-100724/370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**		
Product: nx102-9000					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX10-100724/371
Product: nx102-9020					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration.	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX10-100724/372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33687		
Product: nx1p2-1040dt					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX1P-100724/373
Product: nx1p2-1040dt1					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX1P-100724/374
Product: nx1p2-1140dt					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX1P-100724/375
Product: nx1p2-1140dt1					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX1P-100724/376
Product: nx1p2-9024dt					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all	https://www.fa.omron.co.jp/product/security/assets/pdf/en/	H-OMR-NX1P-100724/377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	OMSR-2024-004_en.pdf	
Product: nx1p2-9024dt1					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX1P-100724/378
Product: nx1w-adb21					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX1W-100724/379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**		
Product: nx1w-cif01					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX1W-100724/380
Product: nx1w-cif11					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration.	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX1W-100724/381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33687		
Product: nx1w-cif12					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX1W-100724/382
Product: nx1w-dab21v					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX1W-100724/383
Product: nx1w-mab221					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX1W-100724/384
Product: nx701-1600					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX70-100724/385
Product: nx701-1620					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all	https://www.fa.omron.co.jp/product/security/assets/pdf/en/	H-OMR-NX70-100724/386

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
			versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	OMSR-2024-004_en.pdf	
Product: nx701-1700					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX70-100724/387
Product: nx701-1720					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX70-100724/388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**		
Product: nx701-z600					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX70-100724/389
Product: nx701-z700					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration.	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	H-OMR-NX70-100724/390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33687		
Vendor: openplcproject					
Product: openplc_v3					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jun-2024	5.4	OpenPLC 3 through 9cd8f1b allows XSS via an SVG document as a profile picture. **CVE ID: CVE-2024-37741**	N/A	H-OPE-OPEN-100724/391
Operating System					
Vendor: hanwhavision					
Product: ane-l6012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-ANE--100724/392

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-2023-5038		
Product: ane-l7012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-ANE--100724/393
Product: ano-l6012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-ANO--100724/394

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: ano-l6022r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-ANO--100724/395
Product: ano-l6082r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					

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
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-ANO--100724/396
Product: ano-l7012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-ANO--100724/397

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: ano-l7022r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-ANO--100724/398
Product: ano-l7082r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-ANO--100724/399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: anv-l6012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-ANV--100724/400

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-2023-5038		
Product: anv-l6023r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-ANV--100724/401
Product: anv-l6082r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-ANV--100724/402

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: anv-l7012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-ANV--100724/403
Product: anv-l7082r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					

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
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-ANV--100724/404
Product: lnd-6012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.13					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-LND--100724/405

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: lnd-6022r_firmware					
Affected Version(s): * Up to (excluding) 1.41.13					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-LND--100724/406
Product: lnd-6032r_firmware					
Affected Version(s): * Up to (excluding) 1.41.13					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-LND--100724/407

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
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: lnd-6072r_firmware					
Affected Version(s): * Up to (excluding) 1.41.13					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-LND--100724/408

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-2023-5038		
Product: lno-6012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.13					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-LNO--100724/409
Product: lno-6022r_firmware					
Affected Version(s): * Up to (excluding) 1.41.13					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-LNO--100724/410

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: lno-6032r_firmware					
Affected Version(s): * Up to (excluding) 1.41.13					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-LNO--100724/411
Product: lno-6072r_firmware					
Affected Version(s): * Up to (excluding) 1.41.13					

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	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-LNO--100724/412
Product: lnv-6012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.13					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-LNV--100724/413

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: lnv-6022r_firmware					
Affected Version(s): * Up to (excluding) 1.41.13					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-LNV--100724/414
Product: lnv-6032r_firmware					
Affected Version(s): * Up to (excluding) 1.41.13					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-LNV--100724/415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: lnv-6072r_firmware					
Affected Version(s): * Up to (excluding) 1.41.13					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-LNV--100724/416

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-2023-5038		
Product: pnm-12082rvd_firmware					
Affected Version(s): * Up to (excluding) 2.22.02					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-PNM--100724/417
Product: pnm-7002vd_firmware					
Affected Version(s): * Up to (excluding) 2.22.02					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-PNM--100724/418

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: pnm-7082rvd_firmware					
Affected Version(s): * Up to (excluding) 2.22.02					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-PNM--100724/419
Product: pnm-8082vt_firmware					
Affected Version(s): * Up to (excluding) 2.22.00					

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	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-PNM--100724/420
Product: pnm-9000qb_firmware					
Affected Version(s): * Up to (excluding) 2.22.01					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-PNM--100724/421

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: pnm-9002vq_firmware					
Affected Version(s): * Up to (excluding) 2.22.02					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-PNM--100724/422
Product: pnm-9022v_firmware					
Affected Version(s): * Up to (excluding) 2.22.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-PNM--100724/423

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
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: pnm-9031rv_firmware					
Affected Version(s): * Up to (excluding) 2.22.01					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-PNM--100724/424

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-2023-5038		
Product: pnm-9084qz1_firmware					
Affected Version(s): * Up to (excluding) 2.22.02					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-PNM--100724/425
Product: pnm-9084qz_firmware					
Affected Version(s): * Up to (excluding) 2.22.02					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-PNM--100724/426

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: pnm-9084rqz1_firmware					
Affected Version(s): * Up to (excluding) 2.22.02					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-PNM--100724/427
Product: pnm-9084rqz_firmware					
Affected Version(s): * Up to (excluding) 2.22.02					

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	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-PNM--100724/428
Product: pnm-9085rqz1_firmware					
Affected Version(s): * Up to (excluding) 2.22.02					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-PNM--100724/429

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: pnm-9085rqz_firmware					
Affected Version(s): * Up to (excluding) 2.22.02					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-PNM--100724/430
Product: pnm-9322vqp_firmware					
Affected Version(s): * Up to (excluding) 2.22.02					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-PNM--100724/431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: pnm-c9022rv_firmware					
Affected Version(s): * Up to (excluding) 2.22.02					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-PNM--100724/432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2023-5038		
Product: qnb-8002_firmware					
Affected Version(s): * Up to (excluding) 1.41.17					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNB--100724/433
Product: qnd-6011_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QND--100724/434

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnd-6012r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QND--100724/435
Product: qnd-6012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					

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
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QND--100724/436
Product: qnd-6021_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QND--100724/437

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnd-6022r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QND--100724/438
Product: qnd-6022r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-QND--100724/439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: qnd-6032r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QND--100724/440

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-2023-5038		
Product: qnd-6032r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QND--100724/441
Product: qnd-6072r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QND--100724/442

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnd-6072r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QND--100724/443
Product: qnd-6073r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					

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
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QND--100724/444
Product: qnd-6082r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QND--100724/445

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnd-6082r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QND--100724/446
Product: qnd-6083r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-QND--100724/447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: qnd-7012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QND--100724/448

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-2023-5038		
Product: qnd-7022r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QND--100724/449
Product: qnd-7032r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QND--100724/450

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnd-7082r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QND--100724/451
Product: qnd-8010r_firmware					
Affected Version(s): * Up to (excluding) 1.42.01					

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	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QND--100724/452
Product: qnd-8011_firmware					
Affected Version(s): * Up to (excluding) 1.42.01					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QND--100724/453

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnd-8020r_firmware					
Affected Version(s): * Up to (excluding) 1.42.01					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QND--100724/454
Product: qnd-8021_firmware					
Affected Version(s): * Up to (excluding) 1.42.01					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-QND--100724/455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: qnd-8030r_firmware					
Affected Version(s): * Up to (excluding) 1.42.01					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QND--100724/456

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-2023-5038		
Product: qnd-8080r_firmware					
Affected Version(s): * Up to (excluding) 1.42.01					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QND--100724/457
Product: qne-8011r_firmware					
Affected Version(s): * Up to (excluding) 1.42.01					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNE--100724/458

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qne-8021r_firmware					
Affected Version(s): * Up to (excluding) 1.42.01					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNE--100724/459
Product: qno-6012r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					

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
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNO--100724/460
Product: qno-6012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNO--100724/461

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qno-6014r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNO--100724/462
Product: qno-6022r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-QNO--100724/463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: qno-6022r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNO--100724/464

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-2023-5038		
Product: qno-6032r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNO--100724/465
Product: qno-6032r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNO--100724/466

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qno-6072r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNO--100724/467
Product: qno-6072r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					

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
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNO--100724/468
Product: qno-6073r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNO--100724/469

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qno-6082r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNO--100724/470
Product: qno-6082r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-QNO--100724/471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: qno-6083r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNO--100724/472

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-2023-5038		
Product: qno-6084r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNO--100724/473
Product: qno-7012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNO--100724/474

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qno-7022r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNO--100724/475
Product: qno-7032r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					

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
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNO--100724/476
Product: qno-7082r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNO--100724/477

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qno-8010r_firmware					
Affected Version(s): * Up to (excluding) 1.42.01					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNO--100724/478
Product: qno-8020r_firmware					
Affected Version(s): * Up to (excluding) 1.42.01					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-QNO--100724/479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: qno-8030r_firmware					
Affected Version(s): * Up to (excluding) 1.42.01					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNO--100724/480

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-2023-5038		
Product: qno-8080r_firmware					
Affected Version(s): * Up to (excluding) 1.42.01					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNO--100724/481
Product: qnv-6012r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNV--100724/482

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnv-6012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNV--100724/483
Product: qnv-6014r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					

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
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNV--100724/484
Product: qnv-6022r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNV--100724/485

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnv-6022r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNV--100724/486
Product: qnv-6023r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-QNV--100724/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: qnv-6024rm_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNV--100724/488

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-2023-5038		
Product: qnv-6032r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNV--100724/489
Product: qnv-6032r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNV--100724/490

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnv-6072r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNV--100724/491
Product: qnv-6072r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					

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
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNV--100724/492
Product: qnv-6073r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNV--100724/493

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnv-6082r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNV--100724/494
Product: qnv-6082r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-QNV--100724/495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: qnv-6083r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNV--100724/496

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-2023-5038		
Product: qnv-6084r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNV--100724/497
Product: qnv-7012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNV--100724/498

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnv-7022r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNV--100724/499
Product: qnv-7032r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					

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
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNV--100724/500
Product: qnv-7082r_firmware					
Affected Version(s): * Up to (excluding) 1.41.16					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNV--100724/501

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: qnv-8010r_firmware					
Affected Version(s): * Up to (excluding) 1.42.01					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNV--100724/502
Product: qnv-8020r_firmware					
Affected Version(s): * Up to (excluding) 1.42.01					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-QNV--100724/503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: qnv-8030r_firmware					
Affected Version(s): * Up to (excluding) 1.42.01					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNV--100724/504

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-2023-5038		
Product: qnv-8080r_firmware					
Affected Version(s): * Up to (excluding) 1.42.01					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-QNV--100724/505
Product: tnv-c7013rc_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-TNV--100724/506

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnb-6002_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNB--100724/507
Product: xnb-6003_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					

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	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNB--100724/508
Product: xnb-8002_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNB--100724/509

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnb-8003_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNB--100724/510
Product: xnb-9002_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-XNB--100724/511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: xnb-9003_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNB--100724/512

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-2023-5038		
Product: xnd-6083rv_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XND--100724/513
Product: xnd-8082rf_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XND--100724/514

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnd-8082rv_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XND--100724/515
Product: xnd-8083rv_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					

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	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XND--100724/516
Product: xnd-8093rv_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XND--100724/517

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnd-9082rf_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XND--100724/518
Product: xnd-9082rv_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-XND--100724/519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: xnd-9083rv_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XND--100724/520

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-2023-5038		
Product: xnd-c6083rv_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XND--100724/521
Product: xnd-c7083rv_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XND--100724/522

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnd-c8083rv_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XND--100724/523
Product: xnd-c9083rv_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					

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	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XND--100724/524
Product: xnf-9010rs_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNF--100724/525

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnf-9010rvm_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNF--100724/526
Product: xnf-9010rv_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-XNF--100724/527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: xnf-9013rv_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNF--100724/528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2023-5038		
Product: xno-6083r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNO--100724/529
Product: xno-6123r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNO--100724/530

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xno-8082r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNO--100724/531
Product: xno-8083r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					

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	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNO--100724/532
Product: xno-9082r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNO--100724/533

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xno-9083r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNO--100724/534
Product: xno-c6083r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-XNO--100724/535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: xno-c7083r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNO--100724/536

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-2023-5038		
Product: xno-c8083r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNO--100724/537
Product: xno-c9083r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNO--100724/538

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnp-6400rw_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNP--100724/539
Product: xnp-6400r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					

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	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNP--100724/540
Product: xnp-6400_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNP--100724/541

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnp-8250r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNP--100724/542
Product: xnp-8250_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-XNP--100724/543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: xnp-8300rw_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNP--100724/544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2023-5038		
Product: xnp-9250r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNP--100724/545
Product: xnp-9250_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNP--100724/546

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnp-9300rw_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNP--100724/547
Product: xnp-c6403rw_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					

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	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNP--100724/548
Product: xnp-c6403r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNP--100724/549

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnp-c6403_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNP--100724/550
Product: xnp-c8253r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-XNP--100724/551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: xnp-c8253_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNP--100724/552

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-2023-5038		
Product: xnp-c8303rw_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNP--100724/553
Product: xnp-c9253r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNP--100724/554

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnp-c9253_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNP--100724/555
Product: xnp-c9303rw_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					

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	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNP--100724/556
Product: xnp-c9310r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNP--100724/557

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnv-6083rz_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNV--100724/558
Product: xnv-6083r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-XNV--100724/559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: xnv-6083z_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNV--100724/560

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-2023-5038		
Product: xnv-6123r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNV--100724/561
Product: xnv-8082r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNV--100724/562

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnv-8083rz_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNV--100724/563
Product: xnv-8083r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					

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	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNV--100724/564
Product: xnv-8083z_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNV--100724/565

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnv-8093r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNV--100724/566
Product: xnv-9082r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-	O-HAN-XNV--100724/567

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
			camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	Vulnerability-Report-CVE-2023-5037-5038.pdf	
Product: xnv-9083rz_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds.	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNV--100724/568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2023-5038		
Product: xnv-9083r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNV--100724/569
Product: xnv-c6083r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNV--100724/570

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
			must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnv-c6083_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNV--100724/571
Product: xnv-c7083r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					

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	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNV--100724/572
Product: xnv-c8083r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNV--100724/573

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
			firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**		
Product: xnv-c9083r_firmware					
Affected Version(s): * Up to (excluding) 2.23.00					
N/A	25-Jun-2024	7.5	badmonkey, a Security Researcher has found a flaw that allows for a unauthenticated DoS attack on the camera. An attacker runs a crafted URL, nobody can access the web management page of the camera. and must manually restart the device or re-power it. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. **CVE ID: CVE-2023-5038**	https://www.hanwhavision.com/wp-content/uploads/2024/06/Camera-Vulnerability-Report-CVE-2023-5037-5038.pdf	O-HAN-XNV--100724/574
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): * Up to (excluding) 2.6.23					
Double Free	24-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/0c02d425a2fbe52643a5859a779db0329e7d	O-LIN-LINU-100724/575

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
			um: Add winch to winch_handlers before registering winch IRQ Registering a winch IRQ is racy, an interrupt may occur before the winch is added to the winch_handlers list. If that happens, register_winch_irq() adds to that list a winch that is scheduled to be (or has already been) freed, causing a panic later in winch_cleanup(). Avoid the race by adding the winch to the winch_handlers list before registering the IRQ, and rolling back if um_request_irq() fails. **CVE ID: CVE-2024-39292**	ddd4, https://git.kernel.org/stable/c/31960d991e43c8d6dc07245f19fc13398e90ead2, https://git.kernel.org/stable/c/351d1a64544944b44732f6a64ed65573b00b9e14	
Affected Version(s): * Up to (excluding) 4.14					
Improper Locking	21-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/165b25e3ee9333f7b04f8db43895beacb515	O-LIN-LINU-100724/576

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
			dma-buf/sw-sync: don't enable IRQ from sync_print_obj() Since commit a6aa8fca4d79 ("dma-buf/sw-sync: Reduce irqsave/irqrestore from known context") by error replaced spin_unlock_irqrestore() with spin_unlock_irq() for both sync_debugfs_show() and sync_print_obj() despite sync_print_obj() is called from sync_debugfs_show(), lockdep complains inconsistent lock state warning. Use plain spin_{lock,unlock}() for sync_print_obj(), for sync_debugfs_show() is already using spin_{lock,unlock}_irq(). **CVE ID: CVE-2024-38780**	82ed, https://git.kernel.org/stable/c/1ff116f68560a25656933d5a18e7619cb6773d8a, https://git.kernel.org/stable/c/242b30466879e6defa521573c27e12018276c33a	
Affected Version(s): * Up to (excluding) 5.11					

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
Out-of-bounds Read	21-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: dma-mapping: benchmark: handle NUMA_NO_NODE correctly cpumask_of_node() can be called for NUMA_NO_NODE inside do_map_benchmark() resulting in the following sanitizer report: UBSAN: array-index-out-of-bounds in ./arch/x86/include/asm/topology.h:72:28 index -1 is out of range for type 'cpumask [64][1]' CPU: 1 PID: 990 Comm: dma_map_benchma Not tainted 6.9.0-rc6 #29 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996) Call Trace: <TASK>	https://git.kernel.org/stable/c/50ee21bfc005e69f183d6b4b454e33f0c2571e1f, https://git.kernel.org/stable/c/5a91116b003175302f2e6ad94b76fb9b5a141a41, https://git.kernel.org/stable/c/8e1ba9df9a35e8dc64f657a64e523c79ba01e464	O-LIN-LINU-100724/577

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
			dump_stack_lvl (lib/dump_stack.c:117) ubsan_epilogue (lib/ubsan.c:232) __ubsan_handle_out_of_bounds (lib/ubsan.c:429) cpumask_of_node (arch/x86/include/asm/topology.h:72) [inline] do_map_benchmark (kernel/dma/map_benchmark.c:104) map_benchmark_ioctl (kernel/dma/map_benchmark.c:246) full_proxy_unlocked_ioctl (fs/debugfs/file.c:333) __x64_sys_ioctl (fs/ioctl.c:890) do_syscall_64 (arch/x86/entry/common.c:83) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) Use cpumask_of_node() in place when binding a kernel thread to a cpuset of a particular node.		

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
			Note that the provided node id is checked inside map_benchmark_ioctl(). It's just a NUMA_NO_NODE case which is not handled properly later. Found by Linux Verification Center (linuxtesting.org). **CVE ID: CVE-2024-39277**		
Affected Version(s): * Up to (excluding) 5.7					
Out-of-bounds Write	24-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: riscv: prevent pt_regs corruption for secondary idle threads Top of the kernel thread stack should be reserved for pt_regs. However this is not the case for the idle threads of the secondary boot harts. Their stacks overlap with their	https://git.kernel.org/stable/c/0c1f28c32a194303da630fca89481334b9547b80, https://git.kernel.org/stable/c/3090c06d50eaa91317f84bf3eac4c265e6cb8d44, https://git.kernel.org/stable/c/a638b0461b58aa3205cd9d5f14d6f703d795b4af	O-LIN-LINU-100724/578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pt_regs, so both may get corrupted. Similar issue has been fixed for the primary hart, see c7cdd96eca28 ("riscv: prevent stack corruption by reserving task_pt_regs(p) early"). However that fix was not propagated to the secondary harts. The problem has been noticed in some CPU hotplug tests with V enabled. The function smp_callin stored several registers on stack, corrupting top of pt_regs structure including status field. As a result, kernel attempted to save or restore inexistent V context. **CVE ID: CVE-2024-38667**		
Affected Version(s): * Up to (excluding) 6.2					
Improper Locking	24-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/6036613570556b5e5ba6d86f505fbc936eff396	O-LIN-LINU-100724/579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drm: zynqmp_dpsub: Always register bridge We must always register the DRM bridge, since zynqmp_dp_hpd_work_func calls drm_bridge_hpd_notify, which in turn expects hpd_mutex to be initialized. We do this before zynqmp_dpsub_drm_init since that calls drm_bridge_attach. This fixes the following lockdep warning: [19.217084] ------------[cut here]------------ [19.227530] DEBUG_LOCKS_WARN_ON(lock->magic != lock) [19.227768] WARNING: CPU: 0 PID: 140 at kernel/locking/mutex.c:582 __mutex_lock+0x4bc/0x550	ba, https://git.kernel.org/stable/c/6ead3eccf67bc8318b1ce95ed879b2cc05b4fce9, https://git.kernel.org/stable/c/be3f3042391d061cfca2bd22630e0d101acea5fc	

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
			[19.241696] Modules linked in: [19.244937] CPU: 0 PID: 140 Comm: kworker/0:4 Not tainted 6.6.20+ #96 [19.252046] Hardware name: xlnx,zynqmp (DT) [19.256421] Workqueue: events zynqmp_dp_hpd_work_func [19.261795] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [19.269104] pc : __mutex_lock+0x4bc/0x550 [19.273364] lr : __mutex_lock+0x4bc/0x550 [19.277592] sp : ffffffc085c5bbe0 [19.281066] x29: ffffffc085c5bbe0 x28: 0000000000000000 x27: ffffff88009417f8 [19.288624] x26: ffffff8800941788 x25: ffffff8800020008 x24: ffffffc082aa3000 [19.296227] x23: ffffffc080d90e3c x22:		

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
			0000000000000002 x21: 0000000000000000 [19.303744] x20: 0000000000000000 x19: ffffff88002f5210 x18: 0000000000000000 [19.311295] x17: 6c707369642e3030 x16: 3030613464662072 x15: 0720072007200720 [19.318922] x14: 0000000000000000 x13: 284e4f5f4e524157 x12: 0000000000000001 [19.326442] x11: 0001ffc085c5b940 x10: 0001ff88003f388b x9 : 0001ff88003f3888 [19.334003] x8 : 0001ff88003f3888 x7 : 0000000000000000 x6 : 0000000000000000 [19.341537] x5 : 0000000000000000 x4 : 000000000000166		

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
			8 x3 : 0000000000000000 [19.349054] x2 : 0000000000000000 x1 : 0000000000000000 x0 : ffffff88003f3880 [19.356581] Call trace: [19.359160] __mutex_lock+0x4bc/0x550 [19.363032] mutex_lock_nested+0x24/0x30 [19.367187] drm_bridge_hpd_notify+0x2c/0x6c [19.371698] zynqmp_dp_hpd_work_func+0x44/0x54 [19.376364] process_one_work+0x3ac/0x988 [19.380660] worker_thread+0x398/0x694 [19.384736] kthread+0x1bc/0x1c0 [19.388241] ret_from_fork+0x10/0x20 [19.392031] irq event stamp: 183 [19.395450] hardirqs last		

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
			enabled at (183): [<ffffffc0800b9278>] finish_task_switch.isra.0+0xa8/0x2d4 [19.405140] hardirqs last disabled at (182): [<ffffffc081ad3754>] __schedule+0x714/0xd04 [19.413612] softirqs last enabled at (114): [<ffffffc080133de8>] srcu_invoke_callbacks+0x158/0x23c [19.423128] softirqs last disabled at (110): [<ffffffc080133de8>] srcu_invoke_callbacks+0x158/0x23c [19.432614] ---[end trace 0000000000000000]--- (cherry picked from commit 61ba791c4a7a09a370c45b70a81b8c7d4cf6b2ae) **CVE ID: CVE-2024-38664**		
Affected Version(s): * Up to (excluding) 6.5					
Buffer Copy	24-Jun-2024	7.8	In the Linux kernel, the following	https://git.kernel.org/stable/c	O-LIN-LINU-100724/580

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
without Checking Size of Input ('Classic Buffer Overflow')			vulnerability has been resolved: drm/amdgpu: Fix buffer size in gfx_v9_4_3_init_ cp_compute_microcode() and rlc_microcode() The function gfx_v9_4_3_init_microcode in gfx_v9_4_3.c was generating about potential truncation of output when using the snprintf function. The issue was due to the size of the buffer 'ucode_prefix' being too small to accommodate the maximum possible length of the string being written into it. The string being written is "amdgpu/%s_mec.bin" or "amdgpu/%s_rlc.bin", where %s is replaced by the value of	/19bd9537b6bc1c882df25206c15917214d8e9460, https://git.kernel.org/stable/c/acce6479e30f73ab0872e93a75aed1fb791d04ec, https://git.kernel.org/stable/c/f1b6a016dfa45cedc080d36fa5d6f22237d80e8b	

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
			'chip_name'. The length of this string without the %s is 16 characters. The warning message indicated that 'chip_name' could be up to 29 characters long, resulting in a total of 45 characters, which exceeds the buffer size of 30 characters. To resolve this issue, the size of the 'ucode_prefix' buffer has been reduced from 30 to 15. This ensures that the maximum possible length of the string being written into the buffer will not exceed its size, thus preventing potential buffer overflow and truncation issues. Fixes the below with gcc W=1: drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c: In function 'gfx_v9_4_3_early_init':		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:379:52: warning: ‘%s’ directive output may be truncated writing up to 29 bytes into a region of size 23 [-Wformat-truncation=] 379 | snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_rlc.bin", chip_name); | ^~ ..... 439 | r = gfx_v9_4_3_init_rlc_microcode(adev, ucode_prefix); | ~~~~~~~~~~~~ drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:379:9: note: ‘snprintf’ output between 16 and 45 bytes into a destination of size 30 379 | snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_rlc.bin", chip_name); | ^~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		

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
			~~ drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:413:52: warning: '%s' directive output may be truncated writing up to 29 bytes into a region of size 23 [-Wformat-truncation=] 413 | snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_mec.bin", chip_name); | ^~ ...... 443 | r = gfx_v9_4_3_init_cp_compute_microcode(adev, ucode_prefix); | ~~~~~~~~~~~~ drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:413:9: note: 'snprintf' output between 16 and 45 bytes into a destination of size 30 413 | snprintf(fw_name, sizeof(fw_name),		

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
			"amdgpu/%s_mec. bin", chip_name); | ^~~~~~~ **CVE ID: CVE-2024-39291**		
Affected Version(s): * Up to (excluding) 6.6					
Improper Check for Unusual or Exceptional Conditions	21-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: tracing/probes: fix error check in parse_btf_field() btf_find_struct_member() might return NULL or an error via the ERR_PTR() macro. However, its caller in parse_btf_field() only checks for the NULL condition. Fix this by using IS_ERR() and returning the error up the stack. **CVE ID: CVE-2024-36481**	https://git.kernel.org/stable/c/4ed468edfeb54c7202e559eba74c25fac6a0dad0, https://git.kernel.org/stable/c/ad4b202da2c498fefb69e5d87f67b946e7fe1e6a, https://git.kernel.org/stable/c/e569eb34970281438e2b48a3ef11c87459fcfbcb	O-LIN-LINU-100724/581
Affected Version(s): * Up to (excluding) 6.6.0					

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
Out-of-bounds Read	21-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: tpm_tis_spi: Account for SPI header when allocating TPM SPI xfer buffer The TPM SPI transfer mechanism uses MAX_SPI_FRAMESIZE for computing the maximum transfer length and the size of the transfer buffer. As such, it does not account for the 4 bytes of header that prepends the SPI data frame. This can result in out-of-bounds accesses and was confirmed with KASAN. Introduce SPI_HDRSIZE to account for the header and use to allocate the transfer buffer.	https://git.kernel.org/stable/c/1547183852dcdfcc25878db7dd3620509217b0cd, https://git.kernel.org/stable/c/195aba96b854dd664768f382cd1db375d8181f88, https://git.kernel.org/stable/c/de13c56f99477b56980c7e00b09c776d16b7563d	O-LIN-LINU-100724/582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-36477		
Affected Version(s): * Up to (excluding) 6.9.4					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: SUNRPC: Fix loop termination condition in gss_free_in_token_pages() The in_token->pages[] array is not NULL terminated. This results in the following KASAN splat: KASAN: maybe wild-memory-access in range [0x04a2013400000008-0x04a201340000000f] **CVE ID: CVE-2024-36288**	https://git.kernel.org/stable/c/0a1cb0c6102bb4fd310243588d39461da49497ad, https://git.kernel.org/stable/c/4a77c3dead97339478c7422eb07bf4bf63577008, https://git.kernel.org/stable/c/4cefcd0af7458bdeff56a9d8dfc6868ce23d128a	O-LIN-LINU-100724/583
Affected Version(s): 6.10.0					
Out-of-bounds Read	21-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: tpm_tis_spi: Account for SPI	https://git.kernel.org/stable/c/1547183852dcdfcc25878db7dd3620509217b0cd, https://git.kernel.org/stable/c	O-LIN-LINU-100724/584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			header when allocating TPM SPI xfer buffer The TPM SPI transfer mechanism uses MAX_SPI_FRAMESIZE for computing the maximum transfer length and the size of the transfer buffer. As such, it does not account for the 4 bytes of header that prepends the SPI data frame. This can result in out-of-bounds accesses and was confirmed with KASAN. Introduce SPI_HDRSIZE to account for the header and use to allocate the transfer buffer. **CVE ID: CVE-2024-36477**	/195aba96b854dd664768f382cd1db375d8181f88, https://git.kernel.org/stable/c/de13c56f99477b56980c7e00b09c776d16b7563d	
Out-of-bounds Read	21-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/50ee21bfc005e69f183d6b4b454e33f0c2571e1f,	O-LIN-LINU-100724/585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dma-mapping: benchmark: handle NUMA_NO_NODE correctly cpumask_of_node() can be called for NUMA_NO_NODE inside do_map_benchmark() resulting in the following sanitizer report: UBSAN: array-index-out-of-bounds in ./arch/x86/include/asm/topology.h:72:28 index -1 is out of range for type 'cpumask [64][1]' CPU: 1 PID: 990 Comm: dma_map_benchma Not tainted 6.9.0-rc6 #29 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996) Call Trace: <TASK> dump_stack_lvl (lib/dump_stack.c:117) ubsan_epilogue (lib/ubsan.c:232)	https://git.kernel.org/stable/c/5a91116b003175302f2e6ad94b76fb9b5a141a41, https://git.kernel.org/stable/c/8e1ba9df9a35e8dc64f657a64e523c79ba01e464	

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
			__ubsan_handle_out_of_bounds (lib/ubsan.c:429) cpumask_of_node (arch/x86/include/asm/topology.h:72) [inline] do_map_benchmark (kernel/dma/map_benchmark.c:104) map_benchmark_ioctl (kernel/dma/map_benchmark.c:246) full_proxy_unlocked_ioctl (fs/debugfs/file.c:333) __x64_sys_ioctl (fs/ioctl.c:890) do_syscall_64 (arch/x86/entry/common.c:83) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) Use cpumask_of_node() in place when binding a kernel thread to a cpuset of a particular node. Note that the provided node id is checked inside map_benchmark_ioctl().		

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 just a NUMA_NO_NODE case which is not handled properly later. Found by Linux Verification Center (linuxtesting.org). **CVE ID: CVE-2024-39277**		
Improper Locking	24-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: drm: zynqmp_dpsub: Always register bridge We must always register the DRM bridge, since zynqmp_dp_hpd_work_func calls drm_bridge_hpd_notify, which in turn expects hpd_mutex to be initialized. We do this before zynqmp_dpsub_drm_init since that calls drm_bridge_attach. This fixes the following lockdep warning:	https://git.kernel.org/stable/c/603661357056b5e5ba6d86f505fbc936eff396ba, https://git.kernel.org/stable/c/6ead3eccf67bc8318b1ce95ed879b2cc05b4fce9, https://git.kernel.org/stable/c/be3f3042391d061cfca2bd22630e0d101acea5fc	O-LIN-LINU-100724/586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[19.217084] ----------[cut here]---------- [19.227530] DEBUG_LOCKS_WARN_ON(lock->magic != lock) [19.227768] WARNING: CPU: 0 PID: 140 at kernel/locking/mutex.c:582 __mutex_lock+0x4bc/0x550 [19.241696] Modules linked in: [19.244937] CPU: 0 PID: 140 Comm: kworker/0:4 Not tainted 6.6.20+ #96 [19.252046] Hardware name: xlnx,zynqmp (DT) [19.256421] Workqueue: events zynqmp_dp_hpd_work_func [19.261795] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [19.269104] pc : __mutex_lock+0x4bc/0x550 [19.273364] lr : __mutex_lock+0x4bc/0x550		

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
			[19.277592] sp : ffffffc085c5bbe0 [19.281066] x29: ffffffc085c5bbe0 x28: 0000000000000000 x27: ffffff88009417f8 [19.288624] x26: ffffff8800941788 x25: ffffff8800020008 x24: ffffffc082aa3000 [19.296227] x23: ffffffc080d90e3c x22: 0000000000000002 x21: 0000000000000000 [19.303744] x20: 0000000000000000 x19: ffffff88002f5210 x18: 0000000000000000 [19.311295] x17: 6c707369642e3030 x16: 3030613464662072 x15: 0720072007200720 [19.318922] x14: 0000000000000000 x13: 284e4f5f4e524157 x12: 0000000000000001		

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
			[19.326442] x11: 0001ffc085c5b940 x10: 0001ff88003f388b x9 : 0001ff88003f3888 [19.334003] x8 : 0001ff88003f3888 x7 : 0000000000000000 x6 : 0000000000000000 [19.341537] x5 : 0000000000000000 x4 : 0000000000001668 x3 : 0000000000000000 [19.349054] x2 : 0000000000000000 x1 : 0000000000000000 x0 : ffffff88003f3880 [19.356581] Call trace: [19.359160] __mutex_lock+0x4bc/0x550 [19.363032] mutex_lock_nested +0x24/0x30 [19.367187] drm_bridge_hpd_notify+0x2c/0x6c [19.371698] zynqmp_dp_hpd_work_func+0x44/0x54		

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
			[19.376364] process_one_work+0x3ac/0x988 [19.380660] worker_thread+0x398/0x694 [19.384736] kthread+0x1bc/0x1c0 [19.388241] ret_from_fork+0x10/0x20 [19.392031] irq event stamp: 183 [19.395450] hardirqs last enabled at (183): [<ffffffc0800b9278>] finish_task_switch.isra.0+0xa8/0x2d4 [19.405140] hardirqs last disabled at (182): [<ffffffc081ad3754>] __schedule+0x714/0xd04 [19.413612] softirqs last enabled at (114): [<ffffffc080133de8>] srcu_invoke_callbacks+0x158/0x23c [19.423128] softirqs last disabled at (110): [<ffffffc080133de8>]		

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
			srcu_invoke_callbacks+0x158/0x23c [19.432614] ---[end trace 0000000000000000]--- (cherry picked from commit 61ba791c4a7a09a370c45b70a81b8c7d4cf6b2ae) **CVE ID: CVE-2024-38664**		
Out-of-bounds Write	24-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: riscv: prevent pt_regs corruption for secondary idle threads Top of the kernel thread stack should be reserved for pt_regs. However this is not the case for the idle threads of the secondary boot harts. Their stacks overlap with their pt_regs, so both may get corrupted. Similar issue has been fixed for the	https://git.kernel.org/stable/c/0c1f28c32a194303da630fca89481334b9547b80, https://git.kernel.org/stable/c/3090c06d50eaa91317f84bf3eac4c265e6cb8d44, https://git.kernel.org/stable/c/a638b0461b58aa3205cd9d5f14d6f703d795b4af	O-LIN-LINU-100724/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			primary hart, see c7cdd96eca28 ("riscv: prevent stack corruption by reserving task_pt_regs(p) early"). However that fix was not propagated to the secondary harts. The problem has been noticed in some CPU hotplug tests with V enabled. The function smp_callin stored several registers on stack, corrupting top of pt_regs structure including status field. As a result, kernel attempted to save or restore inexistent V context. **CVE ID: CVE-2024-38667**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix buffer size in gfx_v9_4_3_init_ cp_compute_microcode() and rlc_microcode()	https://git.kernel.org/stable/c/19bd9537b6bc1c882df25206c15917214d8e9460, https://git.kernel.org/stable/c/acce6479e30f73ab0872e93a75aed1fb791d04ec,	O-LIN-LINU-100724/588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The function gfx_v9_4_3_init_microcode in gfx_v9_4_3.c was generating about potential truncation of output when using the snprintf function. The issue was due to the size of the buffer 'ucode_prefix' being too small to accommodate the maximum possible length of the string being written into it. The string being written is "amdgpu/%s_mec.bin" or "amdgpu/%s_rlc.bin", where %s is replaced by the value of 'chip_name'. The length of this string without the %s is 16 characters. The warning message indicated that 'chip_name' could be up to 29	https://git.kernel.org/stable/c/f1b6a016dfa45cedc080d36fa5d6f22237d80e8b	

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
			characters long, resulting in a total of 45 characters, which exceeds the buffer size of 30 characters. To resolve this issue, the size of the 'ucode_prefix' buffer has been reduced from 30 to 15. This ensures that the maximum possible length of the string being written into the buffer will not exceed its size, thus preventing potential buffer overflow and truncation issues. Fixes the below with gcc W=1: drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c: In function 'gfx_v9_4_3_early_init': drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:379:52: warning: '%s' directive output may be truncated writing up to 29 bytes into a region of size 23 [-		

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
			Wformat-truncation=] 379 | snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_rlc.bin", chip_name); | ^~ ...... 439 | r = gfx_v9_4_3_init_rlc_microcode(adev, ucode_prefix); | ~~~~~~~~~~~~ drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:379:9: note: ‘snprintf’ output between 16 and 45 bytes into a destination of size 30 379 | snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_rlc.bin", chip_name); | ^~~~~~~ drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:413:52: warning: ‘%s’ directive output		

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
			may be truncated writing up to 29 bytes into a region of size 23 [-Wformat-truncation=] 413 | snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_mec.bin", chip_name); | ^~ ...... 443 | r = gfx_v9_4_3_init_cp_compute_microcode(adev, ucode_prefix); | ~~~~~~~~~~~~ drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:413:9: note: ‘snprintf’ output between 16 and 45 bytes into a destination of size 30 413 | snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_mec.bin", chip_name); | ^~~~~~~		

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-2024-39291		
Loop with Unreachable Exit Condition ('Infinite Loop')	21-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: SUNRPC: Fix loop termination condition in gss_free_in_token_pages() The in_token->pages[] array is not NULL terminated. This results in the following KASAN splat: KASAN: maybe wild-memory-access in range [0x04a2013400000008-0x04a201340000000f] **CVE ID: CVE-2024-36288**	https://git.kernel.org/stable/c/0a1cb0c6102bb4fd310243588d39461da49497ad, https://git.kernel.org/stable/c/4a77c3dead97339478c7422eb07bf4bf63577008, https://git.kernel.org/stable/c/4cefcd0af7458bdeff56a9d8dfc6868ce23d128a	O-LIN-LINU-100724/589
Improper Check for Unusual or Exceptional Conditions	21-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: tracing/probes: fix error check in parse_btf_field()	https://git.kernel.org/stable/c/4ed468edfeb54c7202e559eba74c25fac6a0dad0, https://git.kernel.org/stable/c/ad4b202da2c498fefb69e5d87f67b946e7fe1	O-LIN-LINU-100724/590

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
			btf_find_struct_member() might return NULL or an error via the ERR_PTR() macro. However, its caller in parse_btf_field() only checks for the NULL condition. Fix this by using IS_ERR() and returning the error up the stack. **CVE ID: CVE-2024-36481**	e6a, https://git.kernel.org/stable/c/e569eb34970281438e2b48a3ef11c87459fcfbcb	
Improper Locking	21-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: dma-buf/sw-sync: don't enable IRQ from sync_print_obj() Since commit a6aa8fca4d79 ("dma-buf/sw-sync: Reduce irqsave/irqrestore from known context") by error replaced spin_unlock_irqrestore() with spin_unlock_irq() for both sync_debugfs_show() and	https://git.kernel.org/stable/c/165b25e3ee9333f7b04f8db43895beacb51582ed, https://git.kernel.org/stable/c/1ff116f68560a25656933d5a18e7619cb6773d8a, https://git.kernel.org/stable/c/242b30466879e6defa521573c27e12018276c33a	O-LIN-LINU-100724/591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sync_print_obj() despite sync_print_obj() is called from sync_debugfs_show (), lockdep complains inconsistent lock state warning. Use plain spin_{lock,unlock}( ) for sync_print_obj(), for sync_debugfs_show () is already using spin_{lock,unlock}_i rq(). **CVE ID: CVE-2024-38780**		
Double Free	24-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: um: Add winch to winch_handlers before registering winch IRQ Registering a winch IRQ is racy, an interrupt may occur before the winch is added to the winch_handlers list. If that happens, register_winch_irq(	https://git.kernel.org/stable/c/0c02d425a2fbe52643a5859a779db0329e7dddd4, https://git.kernel.org/stable/c/31960d991e43c8d6dc07245f19fc13398e90ead2, https://git.kernel.org/stable/c/351d1a64544944b44732f6a64ed65573b00b9e14	O-LIN-LINU-100724/592

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
			) adds to that list a winch that is scheduled to be (or has already been) freed, causing a panic later in winch_cleanup(). Avoid the race by adding the winch to the winch_handlers list before registering the IRQ, and rolling back if um_request_irq() fails. **CVE ID: CVE-2024-39292**		
N/A	21-Jun-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: bpf: Allow delete from sockmap/sockhash only if update is allowed We have seen an influx of syzkaller reports where a BPF program attached to a tracepoint triggers a locking rule violation by performing a map_delete	https://git.kernel.org/stable/c/000a65bf1dc04fb2b65e2abf116f0bc0fc2ee7b1, https://git.kernel.org/stable/c/11e8ecc5b86037fec43d07b1c162e233e131b1d9, https://git.kernel.org/stable/c/29467edc23818dc5a33042ffb4920b49b090e63d	O-LIN-LINU-100724/593

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
			on a sockmap/sockhash. We don't intend to support this artificial use scenario. Extend the existing verifier allowed-program-type check for updating sockmap/sockhash to also cover deleting from a map. From now on only BPF programs which were previously allowed to update sockmap/sockhash can delete from these map types. **CVE ID: CVE-2024-38662**		
Affected Version(s): From (including) 4.19 Up to (excluding) 4.19.316					
Improper Locking	21-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: dma-buf/sw-sync: don't enable IRQ from sync_print_obj() Since commit a6aa8fca4d79	https://git.kernel.org/stable/c/165b25e3ee9333f7b04f8db43895beacb51582ed, https://git.kernel.org/stable/c/1ff116f68560a25656933d5a18e7619cb6773d8a, https://git.kernel.org/stable/c	O-LIN-LINU-100724/594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			("dma-buf/sw-sync: Reduce irqsave/irqrestore from known context") by error replaced spin_unlock_irqrestore() with spin_unlock_irq() for both sync_debugfs_show() and sync_print_obj() despite sync_print_obj() is called from sync_debugfs_show(), lockdep complains inconsistent lock state warning. Use plain spin_{lock,unlock}() for sync_print_obj(), for sync_debugfs_show() is already using spin_{lock,unlock}_irq(). **CVE ID: CVE-2024-38780**	/242b30466879e6defa521573c27e12018276c33a	
Double Free	24-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: um: Add winch to winch_handlers	https://git.kernel.org/stable/c/0c02d425a2fbe52643a5859a779db0329e7dddd4, https://git.kernel.org/stable/c/31960d991e4	O-LIN-LINU-100724/595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before registering winch IRQ Registering a winch IRQ is racy, an interrupt may occur before the winch is added to the winch_handlers list. If that happens, register_winch_irq( ) adds to that list a winch that is scheduled to be (or has already been) freed, causing a panic later in winch_cleanup(). Avoid the race by adding the winch to the winch_handlers list before registering the IRQ, and rolling back if um_request_irq() fails. **CVE ID: CVE-2024-39292**	3c8d6dc07245f19fc13398e90ead2, https://git.kernel.org/stable/c/351d1a64544944b44732f6a64ed65573b00b9e14	
Affected Version(s): From (including) 5.10 Up to (excluding) 5.10.219					
Improper Locking	21-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: dma-buf/sw-sync: don't enable IRQ	https://git.kernel.org/stable/c/165b25e3ee9333f7b04f8db43895beacb51582ed, https://git.kernel.org/stable/c/1ff116f68560	O-LIN-LINU-100724/596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from sync_print_obj() Since commit a6aa8fca4d79 ("dma-buf/sw-sync: Reduce irqsave/irqrestore from known context") by error replaced spin_unlock_irqrestore() with spin_unlock_irq() for both sync_debugfs_show() and sync_print_obj() despite sync_print_obj() is called from sync_debugfs_show(), lockdep complains inconsistent lock state warning. Use plain spin_{lock,unlock}() for sync_print_obj(), for sync_debugfs_show() is already using spin_{lock,unlock}_irq(). **CVE ID: CVE-2024-38780**	a25656933d5a18e7619cb6773d8a, https://git.kernel.org/stable/c/242b30466879e6defa521573c27e12018276c33a	
Double Free	24-Jun-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/0c02d425a2fb	O-LIN-LINU-100724/597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability has been resolved: um: Add winch to winch_handlers before registering winch IRQ Registering a winch IRQ is racy, an interrupt may occur before the winch is added to the winch_handlers list. If that happens, register_winch_irq() adds to that list a winch that is scheduled to be (or has already been) freed, causing a panic later in winch_cleanup(). Avoid the race by adding the winch to the winch_handlers list before registering the IRQ, and rolling back if um_request_irq() fails. **CVE ID: CVE-2024-39292**	e52643a5859a779db0329e7dddd4, https://git.kernel.org/stable/c/31960d991e43c8d6dc07245f19fc13398e90ead2, https://git.kernel.org/stable/c/351d1a64544944b44732f6a64ed65573b00b9e14	
N/A	21-Jun-2024	4.7	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/000a65bf1dc04fb2b65e2abf1	O-LIN-LINU-100724/598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bpf: Allow delete from sockmap/sockhash only if update is allowed We have seen an influx of syzkaller reports where a BPF program attached to a tracepoint triggers a locking rule violation by performing a map_delete on a sockmap/sockhash. We don't intend to support this artificial use scenario. Extend the existing verifier allowed-program-type check for updating sockmap/sockhash to also cover deleting from a map. From now on only BPF programs which were previously allowed to update	16f0bc0fc2ee7b1, https://git.kernel.org/stable/c/11e8ecc5b86037fec43d07b1c162e233e131b1d9, https://git.kernel.org/stable/c/29467edc23818dc5a33042ffb4920b49b090e63d	

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
			sockmap/sockhash can delete from these map types. **CVE ID: CVE-2024-38662**		
Affected Version(s): From (including) 5.15 Up to (excluding) 5.15.161					
Out-of-bounds Read	21-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: dma-mapping: benchmark: handle NUMA_NO_NODE correctly cpumask_of_node() can be called for NUMA_NO_NODE inside do_map_benchmark() resulting in the following sanitizer report: UBSAN: array-index-out-of-bounds in ./arch/x86/include/asm/topology.h:72:28 index -1 is out of range for type 'cpumask [64][1]' CPU: 1 PID: 990 Comm: dma_map_benchma Not tainted 6.9.0-rc6 #29	https://git.kernel.org/stable/c/50ee21bfc005e69f183d6b4b454e33f0c2571e1f, https://git.kernel.org/stable/c/5a91116b003175302f2e6ad94b76fb9b5a141a41, https://git.kernel.org/stable/c/8e1ba9df9a35e8dc64f657a64e523c79ba01e464	O-LIN-LINU-100724/599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hardware name: QEMU Standard PC (i440FX + PIIX, 1996) Call Trace: <TASK> dump_stack_lvl (lib/dump_stack.c:117) ubsan_epilogue (lib/ubsan.c:232) __ubsan_handle_out_of_bounds (lib/ubsan.c:429) cpumask_of_node (arch/x86/include/asm/topology.h:72) [inline] do_map_benchmark (kernel/dma/map_benchmark.c:104) map_benchmark_ioctl (kernel/dma/map_benchmark.c:246) full_proxy_unlocked_ioctl (fs/debugfs/file.c:333) __x64_sys_ioctl (fs/ioctl.c:890) do_syscall_64 (arch/x86/entry/common.c:83) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130)		

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 cpumask_of_node() in place when binding a kernel thread to a cpuset of a particular node. Note that the provided node id is checked inside map_benchmark_ioctl(). It's just a NUMA_NO_NODE case which is not handled properly later. Found by Linux Verification Center (linuxtesting.org). **CVE ID: CVE-2024-39277**		
Improper Locking	21-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: dma-buf/sw-sync: don't enable IRQ from sync_print_obj() Since commit a6aa8fca4d79 ("dma-buf/sw-sync: Reduce irqsave/irqrestore from	https://git.kernel.org/stable/c/165b25e3ee9333f7b04f8db43895beacb51582ed, https://git.kernel.org/stable/c/1ff116f68560a25656933d5a18e7619cb6773d8a, https://git.kernel.org/stable/c/242b30466879e6defa521573c27e12018276c33a	O-LIN-LINU-100724/600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			known context") by error replaced spin_unlock_irqrestore() with spin_unlock_irq() for both sync_debugfs_show() and sync_print_obj() despite sync_print_obj() is called from sync_debugfs_show(), lockdep complains inconsistent lock state warning. Use plain spin_{lock,unlock}() for sync_print_obj(), for sync_debugfs_show() is already using spin_{lock,unlock}_irq(). **CVE ID: CVE-2024-38780**		
Double Free	24-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: um: Add winch to winch_handlers before registering winch IRQ Registering a winch IRQ is racy, an	https://git.kernel.org/stable/c/0c02d425a2fbe52643a5859a779db0329e7dddd4, https://git.kernel.org/stable/c/31960d991e43c8d6dc07245f19fc13398e90ead2, https://git.kern	O-LIN-LINU-100724/601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interrupt may occur before the winch is added to the winch_handlers list. If that happens, register_winch_irq() adds to that list a winch that is scheduled to be (or has already been) freed, causing a panic later in winch_cleanup(). Avoid the race by adding the winch to the winch_handlers list before registering the IRQ, and rolling back if um_request_irq() fails. **CVE ID: CVE-2024-39292**	el.org/stable/c/351d1a64544944b44732f6a64ed65573b00b9e14	
N/A	21-Jun-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: bpf: Allow delete from sockmap/sockhash only if update is allowed We have seen an influx of syzkaller reports where a	https://git.kernel.org/stable/c/000a65bf1dc04fb2b65e2abf116f0bc0fc2ee7b1, https://git.kernel.org/stable/c/11e8ecc5b86037fec43d07b1c162e233e131b1d9, https://git.kernel.org/stable/c/29467edc23818dc5a33042ff	O-LIN-LINU-100724/602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BPF program attached to a tracepoint triggers a locking rule violation by performing a map_delete on a sockmap/sockhash. We don't intend to support this artificial use scenario. Extend the existing verifier allowed-program-type check for updating sockmap/sockhash to also cover deleting from a map. From now on only BPF programs which were previously allowed to update sockmap/sockhash can delete from these map types. **CVE ID: CVE-2024-38662**	b4920b49b090e63d	
Affected Version(s): From (including) 5.4 Up to (excluding) 5.4.278					
Improper Locking	21-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/165b25e3ee9333f7b04f8db43895beacb51582ed,	O-LIN-LINU-100724/603

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
			dma-buf/sw-sync: don't enable IRQ from sync_print_obj() Since commit a6aa8fca4d79 ("dma-buf/sw-sync: Reduce irqsave/irqrestore from known context") by error replaced spin_unlock_irqrestore() with spin_unlock_irq() for both sync_debugfs_show() and sync_print_obj() despite sync_print_obj() is called from sync_debugfs_show(), lockdep complains inconsistent lock state warning. Use plain spin_{lock,unlock}() for sync_print_obj(), for sync_debugfs_show() is already using spin_{lock,unlock}_irq(). **CVE ID: CVE-2024-38780**	https://git.kernel.org/stable/c/1ff116f68560a25656933d5a18e7619cb6773d8a, https://git.kernel.org/stable/c/242b30466879e6defa521573c27e12018276c33a	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	24-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: um: Add winch to winch_handlers before registering winch IRQ Registering a winch IRQ is racy, an interrupt may occur before the winch is added to the winch_handlers list. If that happens, register_winch_irq() adds to that list a winch that is scheduled to be (or has already been) freed, causing a panic later in winch_cleanup(). Avoid the race by adding the winch to the winch_handlers list before registering the IRQ, and rolling back if um_request_irq() fails. **CVE ID: CVE-2024-39292**	https://git.kernel.org/stable/c/0c02d425a2fbe52643a5859a779db0329e7dddd4, https://git.kernel.org/stable/c/31960d991e43c8d6dc07245f19fc13398e90ead2, https://git.kernel.org/stable/c/351d1a64544944b44732f6a64ed65573b00b9e14	O-LIN-LINU-100724/604
Affected Version(s): From (including) 6.1 Up to (excluding) 6.1.93					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	21-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: dma-mapping: benchmark: handle NUMA_NO_NODE correctly cpumask_of_node() can be called for NUMA_NO_NODE inside do_map_benchmark () resulting in the following sanitizer report: UBSAN: array-index-out-of-bounds in ./arch/x86/include /asm/topology.h:7 2:28 index -1 is out of range for type 'cpumask [64][1]' CPU: 1 PID: 990 Comm: dma_map_benchma Not tainted 6.9.0-rc6 #29 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996) Call Trace: <TASK>	https://git.kernel.org/stable/c/50ee21bfc005e69f183d6b4b454e33f0c2571e1f, https://git.kernel.org/stable/c/5a91116b003175302f2e6ad94b76fb9b5a141a41, https://git.kernel.org/stable/c/8e1ba9df9a35e8dc64f657a64e523c79ba01e464	O-LIN-LINU-100724/605

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
			dump_stack_lvl (lib/dump_stack.c:117) ubsan_epilogue (lib/ubsan.c:232) __ubsan_handle_out_of_bounds (lib/ubsan.c:429) cpumask_of_node (arch/x86/include/asm/topology.h:72) [inline] do_map_benchmark (kernel/dma/map_benchmark.c:104) map_benchmark_ioctl (kernel/dma/map_benchmark.c:246) full_proxy_unlocked_ioctl (fs/debugfs/file.c:333) __x64_sys_ioctl (fs/ioctl.c:890) do_syscall_64 (arch/x86/entry/common.c:83) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) Use cpumask_of_node() in place when binding a kernel thread to a cpuset of a particular node.		

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
			Note that the provided node id is checked inside map_benchmark_ioctl(). It's just a NUMA_NO_NODE case which is not handled properly later. Found by Linux Verification Center (linuxtesting.org). **CVE ID: CVE-2024-39277**		
Out-of-bounds Write	24-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: riscv: prevent pt_regs corruption for secondary idle threads Top of the kernel thread stack should be reserved for pt_regs. However this is not the case for the idle threads of the secondary boot harts. Their stacks overlap with their pt_regs, so both may get corrupted.	https://git.kernel.org/stable/c/0c1f28c32a194303da630fca89481334b9547b80, https://git.kernel.org/stable/c/3090c06d50eaa91317f84bf3eac4c265e6cb8d44, https://git.kernel.org/stable/c/a638b0461b58aa3205cd9d5f14d6f703d795b4af	O-LIN-LINU-100724/606

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
			Similar issue has been fixed for the primary hart, see c7cdd96eca28 ("riscv: prevent stack corruption by reserving task_pt_regs(p) early"). However that fix was not propagated to the secondary harts. The problem has been noticed in some CPU hotplug tests with V enabled. The function smp_callin stored several registers on stack, corrupting top of pt_regs structure including status field. As a result, kernel attempted to save or restore inexistent V context. **CVE ID: CVE-2024-38667**		
Improper Locking	21-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: dma-buf/sw-sync: don't enable IRQ	https://git.kernel.org/stable/c/165b25e3ee9333f7b04f8db43895beacb51582ed, https://git.kernel.org/stable/c/1ff116f68560	O-LIN-LINU-100724/607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from sync_print_obj() Since commit a6aa8fca4d79 ("dma-buf/sw-sync: Reduce irqsave/irqrestore from known context") by error replaced spin_unlock_irqrestore() with spin_unlock_irq() for both sync_debugfs_show() and sync_print_obj() despite sync_print_obj() is called from sync_debugfs_show(), lockdep complains inconsistent lock state warning. Use plain spin_{lock,unlock}() for sync_print_obj(), for sync_debugfs_show() is already using spin_{lock,unlock}_irq(). **CVE ID: CVE-2024-38780**	a25656933d5a18e7619cb6773d8a, https://git.kernel.org/stable/c/242b30466879e6defa521573c27e12018276c33a	
Double Free	24-Jun-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/0c02d425a2fb	O-LIN-LINU-100724/608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability has been resolved: um: Add winch to winch_handlers before registering winch IRQ Registering a winch IRQ is racy, an interrupt may occur before the winch is added to the winch_handlers list. If that happens, register_winch_irq() adds to that list a winch that is scheduled to be (or has already been) freed, causing a panic later in winch_cleanup(). Avoid the race by adding the winch to the winch_handlers list before registering the IRQ, and rolling back if um_request_irq() fails. **CVE ID: CVE-2024-39292**	e52643a5859a779db0329e7dddd4, https://git.kernel.org/stable/c/31960d991e43c8d6dc07245f19fc13398e90ead2, https://git.kernel.org/stable/c/351d1a64544944b44732f6a64ed65573b00b9e14	
N/A	21-Jun-2024	4.7	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/000a65bf1dc04fb2b65e2abf1	O-LIN-LINU-100724/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bpf: Allow delete from sockmap/sockhash only if update is allowed We have seen an influx of syzkaller reports where a BPF program attached to a tracepoint triggers a locking rule violation by performing a map_delete on a sockmap/sockhash. We don't intend to support this artificial use scenario. Extend the existing verifier allowed-program-type check for updating sockmap/sockhash to also cover deleting from a map. From now on only BPF programs which were previously allowed to update	16f0bc0fc2ee7b1, https://git.kernel.org/stable/c/11e8ecc5b86037fec43d07b1c162e233e131b1d9, https://git.kernel.org/stable/c/29467edc23818dc5a33042ffb4920b49b090e63d	

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
			sockmap/sockhash can delete from these map types. **CVE ID: CVE-2024-38662**		
Affected Version(s): From (including) 6.6 Up to (excluding) 6.6.33					
Out-of-bounds Read	21-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: dma-mapping: benchmark: handle NUMA_NO_NODE correctly cpumask_of_node() can be called for NUMA_NO_NODE inside do_map_benchmark() resulting in the following sanitizer report: UBSAN: array-index-out-of-bounds in ./arch/x86/include/asm/topology.h:72:28 index -1 is out of range for type 'cpumask [64][1]' CPU: 1 PID: 990 Comm: dma_map_benchma Not tainted 6.9.0-rc6 #29	https://git.kernel.org/stable/c/50ee21bfc005e69f183d6b4b454e33f0c2571e1f, https://git.kernel.org/stable/c/5a91116b003175302f2e6ad94b76fb9b5a141a41, https://git.kernel.org/stable/c/8e1ba9df9a35e8dc64f657a64e523c79ba01e464	O-LIN-LINU-100724/610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hardware name: QEMU Standard PC (i440FX + PIIX, 1996) Call Trace: <TASK> dump_stack_lvl (lib/dump_stack.c:117) ubsan_epilogue (lib/ubsan.c:232) __ubsan_handle_out_of_bounds (lib/ubsan.c:429) cpumask_of_node (arch/x86/include/asm/topology.h:72) [inline] do_map_benchmark (kernel/dma/map_benchmark.c:104) map_benchmark_ioctl (kernel/dma/map_benchmark.c:246) full_proxy_unlocked_ioctl (fs/debugfs/file.c:333) __x64_sys_ioctl (fs/ioctl.c:890) do_syscall_64 (arch/x86/entry/common.c:83) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130)		

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 cpumask_of_node() in place when binding a kernel thread to a cpuset of a particular node. Note that the provided node id is checked inside map_benchmark_ioctl(). It's just a NUMA_NO_NODE case which is not handled properly later. Found by Linux Verification Center (linuxtesting.org). **CVE ID: CVE-2024-39277**		
Improper Locking	24-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: drm: zynqmp_dpsub: Always register bridge We must always register the DRM bridge, since zynqmp_dp_hpd_work_func calls drm_bridge_hpd_no	https://git.kernel.org/stable/c/603661357056b5e5ba6d86f505fbc936eff396ba, https://git.kernel.org/stable/c/6ead3eccf67bc8318b1ce95ed879b2cc05b4fce9, https://git.kernel.org/stable/c/be3f3042391d061cfca2bd22630e0d101acea5fc	O-LIN-LINU-100724/611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tify, which in turn expects hpd_mutex to be initialized. We do this before zynqmp_dpsub_drm_init since that calls drm_bridge_attach. This fixes the following lockdep warning: [19.217084] ----------[cut here]---------- [19.227530] DEBUG_LOCKS_WARN_ON(lock->magic != lock) [19.227768] WARNING: CPU: 0 PID: 140 at kernel/locking/mutex.c:582 __mutex_lock+0x4bc/0x550 [19.241696] Modules linked in: [19.244937] CPU: 0 PID: 140 Comm: kworker/0:4 Not tainted 6.6.20+ #96 [19.252046] Hardware name: xlnx,zynqmp (DT) [19.256421] Workqueue: events zynqmp_dp_hpd_work_func		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[19.261795] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [19.269104] pc : __mutex_lock+0x4bc/0x550 [19.273364] lr : __mutex_lock+0x4bc/0x550 [19.277592] sp : ffffffc085c5bbe0 [19.281066] x29: ffffffc085c5bbe0 x28: 0000000000000000 x27: ffffff88009417f8 [19.288624] x26: ffffff8800941788 x25: ffffff8800020008 x24: ffffffc082aa3000 [19.296227] x23: ffffffc080d90e3c x22: 0000000000000002 x21: 0000000000000000 [19.303744] x20: 0000000000000000 x19: ffffff88002f5210 x18: 0000000000000000 [19.311295] x17: 6c707369642e303		

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 x16: 3030613464662072 x15: 0720072007200720 [19.318922] x14: 0000000000000000 x13: 284e4f5f4e524157 x12: 0000000000000001 [19.326442] x11: 0001ffc085c5b940 x10: 0001ff88003f388b x9 : 0001ff88003f3888 [19.334003] x8 : 0001ff88003f3888 x7 : 0000000000000000 x6 : 0000000000000000 [19.341537] x5 : 0000000000000000 x4 : 0000000000001668 x3 : 0000000000000000 [19.349054] x2 : 0000000000000000 x1 : 0000000000000000 x0 : ffffff88003f3880 [19.356581] Call trace:		

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
			[19.359160] __mutex_lock+0x4bc/0x550 [19.363032] mutex_lock_nested+0x24/0x30 [19.367187] drm_bridge_hpd_notify+0x2c/0x6c [19.371698] zynqmp_dp_hpd_work_func+0x44/0x54 [19.376364] process_one_work+0x3ac/0x988 [19.380660] worker_thread+0x398/0x694 [19.384736] kthread+0x1bc/0x1c0 [19.388241] ret_from_fork+0x10/0x20 [19.392031] irq event stamp: 183 [19.395450] hardirqs last enabled at (183): [<ffffffc0800b9278>] finish_task_switch.isra.0+0xa8/0x2d4 [19.405140] hardirqs last disabled at (182): [<ffffffc081ad3754>]		

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
			__schedule+0x714/0xd04 [19.413612] softirqs last enabled at (114): [<ffffffc080133de8>] srcu_invoke_callbacks+0x158/0x23c [19.423128] softirqs last disabled at (110): [<ffffffc080133de8>] srcu_invoke_callbacks+0x158/0x23c [19.432614] ---[end trace 0000000000000000]--- (cherry picked from commit 61ba791c4a7a09a370c45b70a81b8c7d4cf6b2ae) **CVE ID: CVE-2024-38664**		
Out-of-bounds Write	24-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: riscv: prevent pt_regs corruption for secondary idle threads Top of the kernel thread stack should	https://git.kernel.org/stable/c/0c1f28c32a194303da630fca89481334b9547b80, https://git.kernel.org/stable/c/3090c06d50eaa91317f84bf3eac4c265e6cb8d44, https://git.kernel.org/stable/c	O-LIN-LINU-100724/612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be reserved for pt_regs. However this is not the case for the idle threads of the secondary boot harts. Their stacks overlap with their pt_regs, so both may get corrupted. Similar issue has been fixed for the primary hart, see c7cdd96eca28 ("riscv: prevent stack corruption by reserving task_pt_regs(p) early"). However that fix was not propagated to the secondary harts. The problem has been noticed in some CPU hotplug tests with V enabled. The function smp_callin stored several registers on stack, corrupting top of pt_regs structure including status field. As a result, kernel attempted to save or restore inexistent V context.	/a638b0461b58aa3205cd9d5f14d6f703d795b4af	

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-2024-38667		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix buffer size in gfx_v9_4_3_init_ cp_compute_microcode() and rlc_microcode() The function gfx_v9_4_3_init_microcode in gfx_v9_4_3.c was generating about potential truncation of output when using the snprintf function. The issue was due to the size of the buffer 'ucode_prefix' being too small to accommodate the maximum possible length of the string being written into it. The string being written is "amdgpu/%s_mec.bin" or	https://git.kernel.org/stable/c/19bd9537b6bc1c882df25206c15917214d8e9460, https://git.kernel.org/stable/c/acce6479e30f73ab0872e93a75aed1fb791d04ec, https://git.kernel.org/stable/c/f1b6a016dfa45cedc080d36fa5d6f22237d80e8b	O-LIN-LINU-100724/613

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
			"amdgpu/%s_rlc.bin", where %s is replaced by the value of 'chip_name'. The length of this string without the %s is 16 characters. The warning message indicated that 'chip_name' could be up to 29 characters long, resulting in a total of 45 characters, which exceeds the buffer size of 30 characters. To resolve this issue, the size of the 'ucode_prefix' buffer has been reduced from 30 to 15. This ensures that the maximum possible length of the string being written into the buffer will not exceed its size, thus preventing potential buffer overflow and truncation issues. Fixes the below with gcc W=1:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c: In function ‘gfx_v9_4_3_early_init’: drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:379:52: warning: ‘%s’ directive output may be truncated writing up to 29 bytes into a region of size 23 [-Wformat-truncation=] 379 | snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_rlc.bin", chip_name); | ^~ ..... 439 | r = gfx_v9_4_3_init_rlc_microcode(adev, ucode_prefix); | ~~~~~~~~~~~~~ drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:379:9: note: ‘snprintf’ output between 16 and 45 bytes into a destination of size 30 379 | snprintf(fw_name, sizeof(fw_name),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			"amdgpu/%s_rlc.bin", chip_name); | ^~~~~~~ drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:413:52: warning: '%s' directive output may be truncated writing up to 29 bytes into a region of size 23 [-Wformat-truncation=] 413 | snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_mec.bin", chip_name); | ^~ ...... 443 | r = gfx_v9_4_3_init_cp_compute_microcode(adev, ucode_prefix); | ~~~~~~~~~~~~ drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:413:9: note: 'snprintf' output between 16 and 45 bytes into a		

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
			destination of size 30 413 | snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_mec.bin", chip_name); | ^~~~~~~ **CVE ID: CVE-2024-39291**		
Improper Locking	21-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: dma-buf/sw-sync: don't enable IRQ from sync_print_obj() Since commit a6aa8fca4d79 ("dma-buf/sw-sync: Reduce irqsave/irqrestore from known context") by error replaced spin_unlock_irqrestore() with spin_unlock_irq() for both sync_debugfs_show() and	https://git.kernel.org/stable/c/165b25e3ee9333f7b04f8db43895beacb51582ed, https://git.kernel.org/stable/c/1ff116f68560a25656933d5a18e7619cb6773d8a, https://git.kernel.org/stable/c/242b30466879e6defa521573c27e12018276c33a	O-LIN-LINU-100724/614

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
			sync_print_obj() despite sync_print_obj() is called from sync_debugfs_show (), lockdep complains inconsistent lock state warning. Use plain spin_{lock,unlock}( ) for sync_print_obj(), for sync_debugfs_show () is already using spin_{lock,unlock}_i rq(). **CVE ID: CVE-2024-38780**		
Double Free	24-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: um: Add winch to winch_handlers before registering winch IRQ Registering a winch IRQ is racy, an interrupt may occur before the winch is added to the winch_handlers list. If that happens, register_winch_irq(	https://git.kernel.org/stable/c/0c02d425a2fbe52643a5859a779db0329e7dddd4, https://git.kernel.org/stable/c/31960d991e43c8d6dc07245f19fc13398e90ead2, https://git.kernel.org/stable/c/351d1a64544944b44732f6a64ed65573b00b9e14	O-LIN-LINU-100724/615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			) adds to that list a winch that is scheduled to be (or has already been) freed, causing a panic later in winch_cleanup(). Avoid the race by adding the winch to the winch_handlers list before registering the IRQ, and rolling back if um_request_irq() fails. **CVE ID: CVE-2024-39292**		
N/A	21-Jun-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: bpf: Allow delete from sockmap/sockhash only if update is allowed We have seen an influx of syzkaller reports where a BPF program attached to a tracepoint triggers a locking rule violation by performing a map_delete	https://git.kernel.org/stable/c/000a65bf1dc04fb2b65e2abf116f0bc0fc2ee7b1, https://git.kernel.org/stable/c/11e8ecc5b86037fec43d07b1c162e233e131b1d9, https://git.kernel.org/stable/c/29467edc23818dc5a33042ffb4920b49b090e63d	O-LIN-LINU-100724/616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on a sockmap/sockhash. We don't intend to support this artificial use scenario. Extend the existing verifier allowed-program-type check for updating sockmap/sockhash to also cover deleting from a map. From now on only BPF programs which were previously allowed to update sockmap/sockhash can delete from these map types. **CVE ID: CVE-2024-38662**		
Affected Version(s): From (including) 6.6.1 Up to (excluding) 6.6.33					
Out-of-bounds Read	21-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: tpm_tis_spi: Account for SPI header when allocating TPM SPI xfer buffer	https://git.kernel.org/stable/c/1547183852dcdfcc25878db7dd3620509217b0cd, https://git.kernel.org/stable/c/195aba96b854dd664768f382cd1db375d8181f88, https://git.kernel.org/stable/c	O-LIN-LINU-100724/617

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 TPM SPI transfer mechanism uses MAX_SPI_FRAMESIZE for computing the maximum transfer length and the size of the transfer buffer. As such, it does not account for the 4 bytes of header that prepends the SPI data frame. This can result in out-of-bounds accesses and was confirmed with KASAN. Introduce SPI_HDRSIZE to account for the header and use to allocate the transfer buffer. **CVE ID: CVE-2024-36477**	/de13c56f99477b56980c7e00b09c776d16b7563d	
Improper Check for Unusual or Exceptional Conditions	21-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: tracing/probes: fix error check in parse_btf_field()	https://git.kernel.org/stable/c/4ed468edfeb54c7202e559eba74c25fac6a0dad0, https://git.kernel.org/stable/c/ad4b202da2c498fefb69e5d87f67b946e7fe1	O-LIN-LINU-100724/618

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
			btf_find_struct_member() might return NULL or an error via the ERR_PTR() macro. However, its caller in parse_btf_field() only checks for the NULL condition. Fix this by using IS_ERR() and returning the error up the stack. **CVE ID: CVE-2024-36481**	e6a, https://git.kernel.org/stable/c/e569eb34970281438e2b48a3ef11c87459fcfbcb	
Affected Version(s): From (including) 6.9 Up to (excluding) 6.9.4					
Out-of-bounds Read	21-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: tpm_tis_spi: Account for SPI header when allocating TPM SPI xfer buffer The TPM SPI transfer mechanism uses MAX_SPI_FRAMESIZE for computing the maximum transfer length and the size of the transfer buffer. As such, it does not account for the 4 bytes of header that	https://git.kernel.org/stable/c/1547183852dcdfcc25878db7dd3620509217b0cd, https://git.kernel.org/stable/c/195aba96b854dd664768f382cd1db375d8181f88, https://git.kernel.org/stable/c/de13c56f99477b56980c7e00b09c776d16b7563d	O-LIN-LINU-100724/619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prepends the SPI data frame. This can result in out-of-bounds accesses and was confirmed with KASAN. Introduce SPI_HDRSIZE to account for the header and use to allocate the transfer buffer. **CVE ID: CVE-2024-36477**		
Out-of-bounds Read	21-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: dma-mapping: benchmark: handle NUMA_NO_NODE correctly cpumask_of_node() can be called for NUMA_NO_NODE inside do_map_benchmark() resulting in the following sanitizer report: UBSAN: array-index-out-of-	https://git.kernel.org/stable/c/50ee21bfc005e69f183d6b4b454e33f0c2571e1f, https://git.kernel.org/stable/c/5a91116b003175302f2e6ad94b76fb9b5a141a41, https://git.kernel.org/stable/c/8e1ba9df9a35e8dc64f657a64e523c79ba01e464	O-LIN-LINU-100724/620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds in ./arch/x86/include/asm/topology.h:72:28 index -1 is out of range for type 'cpumask [64][1]' CPU: 1 PID: 990 Comm: dma_map_benchma Not tainted 6.9.0-rc6 #29 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996) Call Trace: <TASK> dump_stack_lvl (lib/dump_stack.c:117) ubsan_epilogue (lib/ubsan.c:232) __ubsan_handle_out_of_bounds (lib/ubsan.c:429) cpumask_of_node (arch/x86/include/asm/topology.h:72) [inline] do_map_benchmark (kernel/dma/map_benchmark.c:104) map_benchmark_ioctl (kernel/dma/map_benchmark.c:246) full_proxy_unlocked_ioctl		

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
			(fs/debugfs/file.c:333) __x64_sys_ioctl (fs/ioctl.c:890) do_syscall_64 (arch/x86/entry/common.c:83) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) Use cpumask_of_node() in place when binding a kernel thread to a cpuset of a particular node. Note that the provided node id is checked inside map_benchmark_ioctl(). It's just a NUMA_NO_NODE case which is not handled properly later. Found by Linux Verification Center (linuxtesting.org). **CVE ID: CVE-2024-39277**		
Improper Locking	24-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/60366135705 6b5e5ba6d86f5 05fbc936eff396	O-LIN-LINU-100724/621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drm: zynqmp_dpsub: Always register bridge We must always register the DRM bridge, since zynqmp_dp_hpd_work_func calls drm_bridge_hpd_notify, which in turn expects hpd_mutex to be initialized. We do this before zynqmp_dpsub_drm_init since that calls drm_bridge_attach. This fixes the following lockdep warning: [19.217084] ------------[cut here]------------ [19.227530] DEBUG_LOCKS_WARN_ON(lock->magic != lock) [19.227768] WARNING: CPU: 0 PID: 140 at kernel/locking/mutex.c:582 __mutex_lock+0x4bc/0x550	ba, https://git.kernel.org/stable/c/6ead3eccf67bc8318b1ce95ed879b2cc05b4fce9, https://git.kernel.org/stable/c/be3f3042391d061cfca2bd22630e0d101acea5fc	

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
			[19.241696] Modules linked in: [19.244937] CPU: 0 PID: 140 Comm: kworker/0:4 Not tainted 6.6.20+ #96 [19.252046] Hardware name: xlnx,zynqmp (DT) [19.256421] Workqueue: events zynqmp_dp_hpd_work_func [19.261795] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [19.269104] pc : __mutex_lock+0x4bc/0x550 [19.273364] lr : __mutex_lock+0x4bc/0x550 [19.277592] sp : ffffffc085c5bbe0 [19.281066] x29: ffffffc085c5bbe0 x28: 0000000000000000 x27: ffffff88009417f8 [19.288624] x26: ffffff8800941788 x25: ffffff8800020008 x24: ffffffc082aa3000 [19.296227] x23: ffffffc080d90e3c x22:		

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
			0000000000000002 x21: 0000000000000000 [19.303744] x20: 0000000000000000 x19: ffffff88002f5210 x18: 0000000000000000 [19.311295] x17: 6c707369642e3030 x16: 3030613464662072 x15: 0720072007200720 [19.318922] x14: 0000000000000000 x13: 284e4f5f4e524157 x12: 0000000000000001 [19.326442] x11: 0001ffc085c5b940 x10: 0001ff88003f388b x9 : 0001ff88003f3888 [19.334003] x8 : 0001ff88003f3888 x7 : 0000000000000000 x6 : 0000000000000000 [19.341537] x5 : 0000000000000000 x4 : 000000000000166		

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
			8 x3 : 0000000000000000 [19.349054] x2 : 0000000000000000 x1 : 0000000000000000 x0 : ffffff88003f3880 [19.356581] Call trace: [19.359160] __mutex_lock+0x4bc/0x550 [19.363032] mutex_lock_nested+0x24/0x30 [19.367187] drm_bridge_hpd_notify+0x2c/0x6c [19.371698] zynqmp_dp_hpd_work_func+0x44/0x54 [19.376364] process_one_work+0x3ac/0x988 [19.380660] worker_thread+0x398/0x694 [19.384736] kthread+0x1bc/0x1c0 [19.388241] ret_from_fork+0x10/0x20 [19.392031] irq event stamp: 183 [19.395450] hardirqs last		

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
			enabled at (183): [<ffffffc0800b9278>] finish_task_switch.isra.0+0xa8/0x2d4 [19.405140] hardirqs last disabled at (182): [<ffffffc081ad3754>] __schedule+0x714/0xd04 [19.413612] softirqs last enabled at (114): [<ffffffc080133de8>] srcu_invoke_callbacks+0x158/0x23c [19.423128] softirqs last disabled at (110): [<ffffffc080133de8>] srcu_invoke_callbacks+0x158/0x23c [19.432614] ---[end trace 0000000000000000]--- (cherry picked from commit 61ba791c4a7a09a370c45b70a81b8c7d4cf6b2ae) **CVE ID: CVE-2024-38664**		
Out-of-bounds Write	24-Jun-2024	7.8	In the Linux kernel, the following	https://git.kernel.org/stable/c/0c1f28c32a19	O-LIN-LINU-100724/622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability has been resolved: riscv: prevent pt_regs corruption for secondary idle threads Top of the kernel thread stack should be reserved for pt_regs. However this is not the case for the idle threads of the secondary boot harts. Their stacks overlap with their pt_regs, so both may get corrupted. Similar issue has been fixed for the primary hart, see c7cdd96eca28 ("riscv: prevent stack corruption by reserving task_pt_regs(p) early"). However that fix was not propagated to the secondary harts. The problem has been noticed in some CPU hotplug tests with V enabled. The function	4303da630fca89481334b9547b80, https://git.kernel.org/stable/c/3090c06d50eaa91317f84bf3eac4c265e6cb8d44, https://git.kernel.org/stable/c/a638b0461b58aa3205cd9d5f14d6f703d795b4af	

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
			smp_callin stored several registers on stack, corrupting top of pt_regs structure including status field. As a result, kernel attempted to save or restore inexistent V context. **CVE ID: CVE-2024-38667**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix buffer size in gfx_v9_4_3_init_ cp_compute_microcode() and rlc_microcode() The function gfx_v9_4_3_init_microcode in gfx_v9_4_3.c was generating about potential truncation of output when using the snprintf function. The issue was due to the size of the buffer 'ucode_prefix' being too	https://git.kernel.org/stable/c/19bd9537b6bc1c882df25206c15917214d8e9460, https://git.kernel.org/stable/c/acce6479e30f73ab0872e93a75aed1fb791d04ec, https://git.kernel.org/stable/c/f1b6a016dfa45cedc080d36fa5d6f22237d80e8b	O-LIN-LINU-100724/623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			small to accommodate the maximum possible length of the string being written into it. The string being written is "amdgpu/%s_mec.bin" or "amdgpu/%s_rlc.bin", where %s is replaced by the value of 'chip_name'. The length of this string without the %s is 16 characters. The warning message indicated that 'chip_name' could be up to 29 characters long, resulting in a total of 45 characters, which exceeds the buffer size of 30 characters. To resolve this issue, the size of the 'ucode_prefix' buffer has been reduced from 30 to 15. This ensures that the maximum possible length of		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the string being written into the buffer will not exceed its size, thus preventing potential buffer overflow and truncation issues. Fixes the below with gcc W=1: drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c: In function 'gfx_v9_4_3_early_init': drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:379:52: warning: '%s' directive output may be truncated writing up to 29 bytes into a region of size 23 [-Wformat-truncation=] 379 | snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_rlc.bin", chip_name); | ^~ ..... 439 | r = gfx_v9_4_3_init_rlc_microcode(adev, ucode_prefix);		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			| ~~~~~~~~~~~~~ drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:379:9: note: 'snprintf' output between 16 and 45 bytes into a destination of size 30 379 | snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_rlc.bin", chip_name); | ^~~~~~~ drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:413:52: warning: '%s' directive output may be truncated writing up to 29 bytes into a region of size 23 [-Wformat-truncation=] 413 | snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_mec.bin", chip_name); | ^~		

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
			443 | r = gfx_v9_4_3_init_cp_compute_microcode(adev, ucode_prefix); | ~~~~~~~~~~~~~ drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:413:9: note: 'snprintf' output between 16 and 45 bytes into a destination of size 30 413 | snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_mec.bin", chip_name); | ^~~~~~~~~~~~ ~~~~~~~~~~~~ ~~~~~~~~~~~~ ~~~~~~~~~~~~ ~~~~~~~~~~~~ ~~~~~~ **CVE ID: CVE-2024-39291**		
Improper Check for Unusual or Exceptional Conditions	21-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: tracing/probes: fix error check in parse_btf_field() btf_find_struct_member() might	https://git.kernel.org/stable/c/4ed468edfeb54c7202e559eba74c25fac6a0dad0, https://git.kernel.org/stable/c/ad4b202da2c498fefb69e5d87f67b946e7fe1e6a, https://git.kern	O-LIN-LINU-100724/624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			return NULL or an error via the ERR_PTR() macro. However, its caller in parse_btf_field() only checks for the NULL condition. Fix this by using IS_ERR() and returning the error up the stack. **CVE ID: CVE-2024-36481**	el.org/stable/c/e569eb34970281438e2b48a3ef11c87459fcfbcb	
Improper Locking	21-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: dma-buf/sw-sync: don't enable IRQ from sync_print_obj() Since commit a6aa8fca4d79 ("dma-buf/sw-sync: Reduce irqsave/irqrestore from known context") by error replaced spin_unlock_irqrestore() with spin_unlock_irq() for both sync_debugfs_show() and sync_print_obj() despite	https://git.kernel.org/stable/c/165b25e3ee9333f7b04f8db43895beacb51582ed, https://git.kernel.org/stable/c/1ff116f68560a25656933d5a18e7619cb6773d8a, https://git.kernel.org/stable/c/242b30466879e6defa521573c27e12018276c33a	O-LIN-LINU-100724/625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sync_print_obj() is called from sync_debugfs_show(), lockdep complains inconsistent lock state warning. Use plain spin_{lock,unlock}() for sync_print_obj(), for sync_debugfs_show() is already using spin_{lock,unlock}_irq(). **CVE ID: CVE-2024-38780**		
Double Free	24-Jun-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: um: Add winch to winch_handlers before registering winch IRQ Registering a winch IRQ is racy, an interrupt may occur before the winch is added to the winch_handlers list. If that happens, register_winch_irq() adds to that list a winch that is	https://git.kernel.org/stable/c/0c02d425a2fbe52643a5859a779db0329e7dddd4, https://git.kernel.org/stable/c/31960d991e43c8d6dc07245f19fc13398e90ead2, https://git.kernel.org/stable/c/351d1a64544944b44732f6a64ed65573b00b9e14	O-LIN-LINU-100724/626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scheduled to be (or has already been) freed, causing a panic later in winch_cleanup(). Avoid the race by adding the winch to the winch_handlers list before registering the IRQ, and rolling back if um_request_irq() fails. **CVE ID: CVE-2024-39292**		
N/A	21-Jun-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: bpf: Allow delete from sockmap/sockhash only if update is allowed We have seen an influx of syzkaller reports where a BPF program attached to a tracepoint triggers a locking rule violation by performing a map_delete on a sockmap/sockhash.	https://git.kernel.org/stable/c/000a65bf1dc04fb2b65e2abf116f0bc0fc2ee7b1, https://git.kernel.org/stable/c/11e8ecc5b86037fec43d07b1c162e233e131b1d9, https://git.kernel.org/stable/c/29467edc23818dc5a33042ffb4920b49b090e63d	O-LIN-LINU-100724/627

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
			We don't intend to support this artificial use scenario. Extend the existing verifier allowed-program-type check for updating sockmap/sockhash to also cover deleting from a map. From now on only BPF programs which were previously allowed to update sockmap/sockhash can delete from these map types. **CVE ID: CVE-2024-38662**		
Vendor: Omron					
Product: nj-pa3001_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ-P-100724/628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			detect the alteration. **CVE ID: CVE-2024-33687**		
Product: nj-pd3001_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ-P-100724/629
Product: nj101-1000_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ10-100724/630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nj101-1020_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ10-100724/631
Product: nj101-9000_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ10-100724/632
Product: nj101-9020_firmware					
Affected Version(s): *					
Insufficient Verificatio	24-Jun-2024	7.5	Insufficient verification of data	https://www.fa.omron.co.jp/pr	O-OMR-NJ10-100724/633

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 of Data Authenticity			authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	oduct/security/assets/pdf/en/OMSR-2024-004_en.pdf	
Product: nj301-1100_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ30-100724/634
Product: nj301-1200_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ30-100724/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**		
Product: nj501-1300_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ50-100724/636
Product: nj501-1320_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ50-100724/637

* Stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			detect the alteration. **CVE ID: CVE-2024-33687**		
Product: nj501-1340_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ50-100724/638
Product: nj501-1400_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ50-100724/639

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: nj501-140_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ50-100724/640
Product: nj501-1420_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ50-100724/641
Product: nj501-1500_firmware					
Affected Version(s): *					
Insufficient Verificatio	24-Jun-2024	7.5	Insufficient verification of data	https://www.fa.omron.co.jp/pr	O-OMR-NJ50-100724/642

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 of Data Authenticity			authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	oduct/security/assets/pdf/en/OMSR-2024-004_en.pdf	
Product: nj501-1520_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ50-100724/643
Product: nj501-4300_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ50-100724/644

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
			versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**		
Product: nj501-4310_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ50-100724/645
Product: nj501-4320_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ50-100724/646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			detect the alteration. **CVE ID: CVE-2024-33687**		
Product: nj501-4400_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ50-100724/647
Product: nj501-4500_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ50-100724/648

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: nj501-5300-1_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ50-100724/649
Product: nj501-5300_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ50-100724/650
Product: nj501-r300_firmware					
Affected Version(s): *					
Insufficient Verificatio	24-Jun-2024	7.5	Insufficient verification of data	https://www.fa.omron.co.jp/pr	O-OMR-NJ50-100724/651

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 of Data Authenticity			authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	oduct/security/assets/pdf/en/OMSR-2024-004_en.pdf	
Product: nj501-r320_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ50-100724/652
Product: nj501-r400_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ50-100724/653

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
			versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**		
Product: nj501-r420_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ50-100724/654
Product: nj501-r500_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ50-100724/655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			detect the alteration. **CVE ID: CVE-2024-33687**		
Product: nj501-r520_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NJ50-100724/656
Product: nx102-1000_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX10-100724/657

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: nx102-1020_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX10-100724/658
Product: nx102-1100_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX10-100724/659
Product: nx102-1120_firmware					
Affected Version(s): *					
Insufficient Verificatio	24-Jun-2024	7.5	Insufficient verification of data	https://www.fa.omron.co.jp/pr	O-OMR-NX10-100724/660

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 of Data Authenticity			authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	oduct/security/assets/pdf/en/OMSR-2024-004_en.pdf	
Product: nx102-1200_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX10-100724/661
Product: nx102-1220_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX10-100724/662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**		
Product: nx102-9000_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX10-100724/663
Product: nx102-9020_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX10-100724/664

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
			detect the alteration. **CVE ID: CVE-2024-33687**		
Product: nx1p2-1040dt1_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX1P-100724/665
Product: nx1p2-1040dt_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX1P-100724/666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nx1p2-1140dt1_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX1P-100724/667
Product: nx1p2-1140dt_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX1P-100724/668
Product: nx1p2-9024dt1_firmware					
Affected Version(s): *					
Insufficient Verificatio	24-Jun-2024	7.5	Insufficient verification of data	https://www.fa.omron.co.jp/pr	O-OMR-NX1P-100724/669

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 of Data Authenticity			authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	oduct/security/assets/pdf/en/OMSR-2024-004_en.pdf	
Product: nx1p2-9024dt_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX1P-100724/670
Product: nx1w-adb21_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX1W-100724/671

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
			versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**		
Product: nx1w-cif01_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX1W-100724/672
Product: nx1w-cif11_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX1W-100724/673

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
			detect the alteration. **CVE ID: CVE-2024-33687**		
Product: nx1w-cif12_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX1W-100724/674
Product: nx1w-dab21v_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX1W-100724/675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nx1w-mab221_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX1W-100724/676
Product: nx701-1600_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX70-100724/677
Product: nx701-1620_firmware					
Affected Version(s): *					
Insufficient Verificatio	24-Jun-2024	7.5	Insufficient verification of data	https://www.fa.omron.co.jp/pr	O-OMR-NX70-100724/678

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 of Data Authenticity			authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	oduct/security/assets/pdf/en/OMSR-2024-004_en.pdf	
Product: nx701-1700_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX70-100724/679
Product: nx701-1720_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX70-100724/680

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
			versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**		
Product: nx701-z600_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to detect the alteration. **CVE ID: CVE-2024-33687**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX70-100724/681
Product: nx701-z700_firmware					
Affected Version(s): *					
Insufficient Verification of Data Authenticity	24-Jun-2024	7.5	Insufficient verification of data authenticity issue exists in NJ Series CPU Unit all versions and NX Series CPU Unit all versions. If a user program in the affected product is altered, the product may not be able to	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-004_en.pdf	O-OMR-NX70-100724/682

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
			detect the alteration. **CVE ID: CVE-2024-33687**		
Vendor: openplcproject					
Product: openplc_v3_firmware					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jun-2024	5.4	OpenPLC 3 through 9cd8f1b allows XSS via an SVG document as a profile picture. **CVE ID: CVE-2024-37741**	N/A	O-OPE-OPEN-100724/683
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 7.0					
N/A	21-Jun-2024	7.5	A flaw was found in the Poppler's Pdfinfo utility. This issue occurs when using -dests parameter with pdfinfo utility. By using certain malformed input files, an attacker could cause the utility to crash, leading to a denial of service. **CVE ID: CVE-2024-6239**	https://bugzilla.redhat.com/show_bug.cgi?id=2293594	O-RED-ENTE-100724/684
Affected Version(s): 8.0					
N/A	21-Jun-2024	7.5	A flaw was found in the Poppler's Pdfinfo utility. This issue occurs when using -dests	https://bugzilla.redhat.com/show_bug.cgi?id=2293594	O-RED-ENTE-100724/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter with pdfinfo utility. By using certain malformed input files, an attacker could cause the utility to crash, leading to a denial of service. **CVE ID: CVE-2024-6239**		
Affected Version(s): 9.0					
N/A	21-Jun-2024	7.5	A flaw was found in the Poppler's Pdfinfo utility. This issue occurs when using -dests parameter with pdfinfo utility. By using certain malformed input files, an attacker could cause the utility to crash, leading to a denial of service. **CVE ID: CVE-2024-6239**	https://bugzilla.redhat.com/show_bug.cgi?id=2293594	O-RED-ENTE-100724/686

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